Enhancing the security of wireless sensor network based home automation systems

Loughborough University

Thesis Access Form

Copy No……..…….**Location**…….……...…

Author Khusvinder Gill

Title "Enhancing the Security of Wireless Sensor Network based Home Automation Systems"

Status of access OPEN / RESTRICTED / CONFIDENTIAL

Moratorium Period:……years,
ending……../……200…….

Conditions of access approved by (CAPITALS):……

Supervisor (Signature)……...……...

Department of Computer Science

Author's Declaration: *I agree the following conditions:*

Open access work shall be made available (in the University and externally) and reproduced as necessary at the discretion of the University Librarian or Head of Department. It may also be digitised by the British Library and made freely available on the Internet to registered users of the EThOS service subject to the EThOS supply agreements.

*The statement itself shall apply to **ALL** copies including electronic copies:*

This copy has been supplied on the understanding that it is copyright material and that no quotation from the thesis may be published without proper acknowledgement.

Restricted/confidential work: All access and any photocopying shall be strictly subject to written permission from the University Head of Department and any external sponsor, if any.

Author's signature……Date……...…

users declaration: for signature during any Moratorium period (Not Open work): ***I undertake to uphold the above conditions:***			
Date	Name (CAPITALS)	Signature	Address

Enhancing the Security of Wireless Sensor Network based Home Automation Systems

by

Khusvinder Gill

A Doctoral Thesis

Submitted in partial fulfilment

of the requirements for the award of

Doctor of Philosophy

Of

Loughborough University

October 2009

Certificate of Originality

This is to certify that I am responsible for the work submitted in this thesis, that the original work is my own except as specified in acknowledgments or in footnotes, and that neither the thesis nor the original work contained therein has been submitted to this or any other institution for a higher degree.

Author's signature ……

Date ……

Acknowledgments

A number of people have supported me throughout my research. The following acknowledgments go a small way to expressing my thanks.

Firstly, I would like to thank my academic supervisor Professor Shuang-Hua Yang and my director of research Dr. Serpil Acar for their continued guidance, and support. They provided me with the motivation I needed to focus and achieve my goals.

A number of members of staff from the Computer Science department have provided assistance over the last three years. I would like to thank Gurbinder Singh Samra, Christine Bagley, Judith Poulton, Roger Knott, and Kip Sahnsi for doing their best to help, and always doing so with a smile.

My father, Sarabjit, my mother Manjit and my sister Amandeep have supported and encouraged me throughout my life. This has been especially true during my PhD, without their love and encouragement the PhD would not have been possible.

I would like to thank: Nijad Al-Najdawi for keeping me distracted with all the bargain hunting and barbeques. Sara Tedmori for all the coffee and lunch breaks, for being such a caring friend and making my time at Holywell more enjoyable. Yara Al-Najdawi for cheering me up during the hardest periods of my PhD, by being such an adorable baby, even from afar. Ashraf Al-Najdawi for all the late dinners and his continued friendship.

My life at Loughborough has been shared with Hesham Abusaimeh and Tareq Alhmiedat for the last three years, lunch times will not be the same without you guys, I could not have asked for better friends. I would like to express my gratitude to Amr Sourani for making some of the late nights at Holywell fun and Nuha Alfarra for being such a good friend.

Finally, I would like to thank all of my friends at Holywell park for constantly reminding me that there is more to life than work, and continuing to do so even when I didn't always listen. Special thanks goes to Lezan Hawizy, Alexandra Alecu, Scott Culcheth, Martin Sykora, Mark Withall, Matthew Atkinson, Jatinder Gill, Yao Fang, Yunqiu Li (Karen), Yanning Yang, Senay Mihcen, Huanjia Yang, Xin Lu, Zaid Bin Ahmad, Ran Xu, Steve Smith , and Carlos Insaurralde.

Thank you all.

Abstract

Home automation systems (HASs) seek to improve the quality of life for individuals through the automation of household devices. Recently, there has been a trend, in academia and industry, to research and develop low-cost Wireless Sensor Network (WSN) based HASs (Varchola et al. 2007). WSNs are designed to achieve a low-cost wireless networking solution, through the incorporation of limited processing, memory, and power resources. Consequently, providing secure and reliable remote access for resource limited WSNs, such as WSN based HASs, poses a significant challenge (Perrig et al. 2004).

This thesis introduces the development of a hybrid communications approach to increase the resistance of WSN based HASs to remote DoS flooding attacks targeted against a third party. The approach is benchmarked against the dominant GHS remote access approach for WSN based HASs (Bergstrom et al. 2001), on a WSN based HAS test-bed, and shown to provide a minimum of a 58.28%, on average 59.85%, and a maximum of 61.45% increase in remote service availability during a DoS attack. Additionally, a virtual home incorporating a cryptographic based DoS detection algorithm, is developed to increase resistance to remote DoS flooding attacks targeted directly at WSN based HASs. The approach is benchmarked against D-WARD (Mirkovic 2003), the most effective DoS defence identified from the research, and shown to provide a minimum 84.70%, an average 91.13% and a maximum 95.6% reduction in packets loss on a WSN based HAS during a DoS flooding attack. Moreover, the approach is extended with the integration of a virtual home, hybrid communication approach, and a distributed denial of defence server to increase resistance to remote DoS attacks targeting the home gateway. The approach is again benchmarked against the D-WARD defence and shown to decrease the connection latency experienced by remote users by a minimum of 90.14%, an average 90.90%, and a maximum 91.88%

Keywords: Denial of Service, Wireless Sensor Networks, Home Automation, Remote Access, Security.

Publications

Journal Publications

Gill, K., Yang, S., Yao, F., and Lu, X., "A Zigbee-based home automation system", *IEEE Transactions on Consumer Electronics*, 55(2), pp.422-430, May 2009.

Gill, K. and Yang, S., "Home Automation Systems - Secure Remote Access", *Measurement + Control*, 41(10), pp. 305-309, December 2008.

Conference Publications

Gill, K. and Yang, S., "A Scheme for Preventing Denial of Service Attacks on Wireless Sensor Networks", *the Proceedings of the 35th Annual Conference of the IEEE Industrial Electronics Society*, Oporto, Portugal, pp. 2623-2629, November 2009.

Gill, K., Yao, F., and Yang, S., "Transparent Heterogeneous Networks for the Remote Control of Home Environments", *the Proceedings of the 2008 IEEE International Conference On Networking, Sensing and Control*, Sanya, China, pp. 1419-1424, April 2008.

Gill, K., Yao, F., and Yang, S., "The Design and Implementation of a Flexible Home Gateway Architecture", *The 13th International Conference on Automation and Computing*, Staffordshire, UK, pp. 128-133, September 2007.

Yao, F., Gill, K., and Yang, S., "A Zibee Based Low Cost Home Automation System", *The 13th International Conference on Automation and Computing*, Staffordshire, UK, pp. 258-263, September 2007.

Journal Papers Under Review

Gill, K. and Yang, S., "A Scheme for Preventing Low-Level Denial of Service Attacks on Wireless Sensor Networks", *IEEE Transactions on Consumer Electronics.*

Gill, K. and Yang, S., "An Approach for Secure Remote Access to Wireless Sensor Network based Home Automation Systems", *IEEE Communications Magazine*.

Abbreviations

ACC	:	Aggregate Congestion Control
ACK	:	Acknowledgement Packet
ACP	:	Active Security Protocol
ADSL	:	Asymmetric Digital Subscriber Line
AES	:	Advanced Encryption Standard
API	:	Application Programming Interface
APL	:	Application Layer
APO	:	Application Object
APS	:	Application Support Sublayer
ASSYST	:	Active Security System
BBC	:	British Broadcasting Corporation
B-MAC	:	Berkley Medium Access Control Protocol
CAP	:	Contention Access Period
CBC	:	Cipher Block Chaining

CCA	:	Clear Channel Assessment
CCM*	:	Counter with CBC-MAC
CEBus	:	Consumer Electronics Bus
CFP	:	Contention Free Period
CPU	:	Central Processing Unit
CSMA – CA	:	Carrier Sense Multiple Access with Collision Avoidance
CTR	:	Counter
CTS	:	Clear to Send
DDoS	:	Distributed Denial of Service
DDS	:	DoS Defence Server
DES	:	Digital Encryption Standard
DNS	:	Domain Name Server
DoS	:	Denial of Service
DPF	:	Distributed Packet Filtering
DVD	:	Digital Versatile Disc
D-WARD	:	DDoS Network Attack Recognition and Defence
ECB	:	Electronic Codebook
EIB	:	European Installation Bus
EPOS	:	Electronic Point of Sale
FFD	:	Full Function Device

FIN	:	Finish Packet
FRTS	:	Future Request to Send
FSK	:	Frequency Shift Keying
FTP	:	File Transfer Protocol
GHS	:	Global Home Server
G-MAC	:	Gateway Medium Access Control Protocol
GPS	:	Global Positioning System
GSM	:	Global System for Mobile Communications
GTIM	:	Gateway Traffic Indication Message
GTS	:	Guaranteed Time Slots
HA	:	Housing Association
HAS	:	Home Automation System
HTML	:	Hyper Text Markup Language
HTTP	:	Hypertext Transfer Protocol
IEEE	:	Institute of Electrical and Electronic Engineers
ICMP	:	Internet Control Message Protocol
IP	:	Internet Protocol
IPv4	:	Internet Protocol version 4
IPv6	:	Internet Protocol version 6
ISM	:	Industrial, Scientific, and Medical
ISO	:	International Organisation for Standardisation

ISP	:	Internet Service Provider
ITU	:	International Telecommunications Union
ITU-T	:	ITU Telecommunications Standardisation Sector
J2ME	:	Java 2 Platform, Micro Edition
KNX	:	Konnex
LAN	:	Local Area Network
LR-WPAN	:	Low Rate Wireless Personal Area Network
LQI	:	Link Quality Indicator
MAC	:	Medium Access Control Message Authentication Code
MAN	:	Metropolitan Area Network
MIPS	:	Microprocessor without Interlocked Pipeline Stages
MULTOPS	:	Multi-level Tree for online Packet Statistics
NAT	:	Network Address Translation
NID	:	Network based Intrusion Detection
NWK	:	Network Layer
OSI	:	Open Systems Interconnection
PAN	:	Personal Area Network
PAN ID	:	Personal Area Network Identifier
PDA	:	Personal Digital Assistant

PHY	:	Physical Layer
PKC	:	Public Key Cryptography
PPM	:	Packets Per Minute
QoS	:	Quality of Service
RAM	:	Random Access Memory
RF	:	Radio Frequency
RFD	:	Reduced Function Device
RHS	:	Remote Home Server
RISC	:	Reduced Instruction Set Computer
ROM	:	Read Only Memory
RPF	:	Route based Packet Filtering
RST	:	Reset Packet
RTS	:	Request to Send
SIDS	:	Sudden Infant Death Syndrome
S-MAC	:	Sensor Medium Access Control Protocol
SMTP	:	Simple Mail Transfer Protocol
SOAP	:	Secure Overlay Access Point
SOS	:	Secure Overlay Service
SQL	:	Structured Query Language
SSL	:	Secure Sockets Layer
SYN	:	Synchronisation Packet

TCP	:	Transmission Control Protocol
T-MAC	:	Timeout Medium Access Control Protocol
TRV	:	Thermostatic Radiator Valve
TSB	:	Technology Strategy Board
UDP	:	User Datagram Protocol
UK	:	United Kingdom
VH	:	Virtual Home
VPN	:	Virtual Private Network
WAN	:	Wide Area Network
WSN	:	Wireless Sensor Network
WWW	:	World Wide Web
ZDO	:	ZigBee Device Object

List of Symbols

DE	:	Number of decryption errors in a given minute
DF	:	Number of decryption failures in a given minute
f(x)	:	Represents a generic symmetric encryption and decryption function
Gbps	:	Giga bits per second
GHz	:	Gigahertz
IPx	:	Number of seconds after which a home updates the IP address held by a third party
Kbps	:	Kilo bits per second
Kc	:	Client master key
kHz	:	Kilohertz
km	:	Kilometre
Km	:	Server master key
Ks	:	Session Key

m	:	Meter
M	:	Message
Mbps	:	Mega bits per second
MHz	:	Megahertz
ms	:	Milliseconds
n	:	Hash Value
N	:	Nonce
RM	:	Number of replayed messages in a given minute
SKx	:	Number of messages after which the session key is refreshed

Table of Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Background to the Research

Over the last two decades, there has been an exponential growth in the number of computers. In parallel with the rapid adoption of computers, large networks such as the Internet have emerged as a popular means to exchange data and information between computerised devices (Tanenbaum 2003).

Recent developments in technology have seen an increase in the range and diversity of computers used in industry and by consumers. Computer technology in the consumer domain is no longer limited to personal computers occupying fixed desk space in offices and bedrooms. Instead, there has been an increasing trend towards ubiquitous computing, where by computers integrate seamlessly into the peripheral environment to assist and provide services for users. Often users are not aware of the computers and networks operating in the environment, working together to provide them with services (Hawizy 2007).

WSNs are an emerging technology for providing intelligent ubiquitous computing environments. WSNs consists of low cost, resource limited sensor nodes that can be randomly distributed across areas of varying sizes to autonomously form wireless networks (Tanenbaum 2003). WSN nodes monitor their surrounding environment and share information collected with other nodes in the same network.

Sensed information is used by devices connected to the WSN to provide tailored services that are responsive to environmental changes.

Through integration with existing networks, such as the Internet, WSNs have created the potential for many new applications (Baker et al. 2007). The scope for potential WSN based applications is enormous, existing applications include, patient monitoring in hospitals, tracking of military ordinance, location tracking, environmental monitoring in extreme or remote locations such as near volcanoes or in the tropical rainforest respectively, and home automation (Akyildiz et al. 2002).

The work outlined in this thesis primarily focuses on WSN based HASs. There are many definitions of home automation available in the literature. (Bromley et al. 2003) describes home automation as the introduction of technology within the home to enhance the quality of life of its occupants, through the provision of different services such as telehealth, multimedia entertainment and energy conservation.

The introduction of WSN based HASs offers the potential for new applications (Baker et al. 2007), however significant challenges also arise, primarily due to the resource-limited nature of WSNs. One of the greatest challenges to have emerged is that of providing sufficient security for the creation of secure and reliable WSNs, such as WSN based HAS, with the limited resources available (Perrig et al. 2004). As identified from the literature review (see Chapter 3) most of the existing research reviewed, related to the reliability of WSNs, focuses on protecting the availability of WSNs from DoS attacks originating from within the WSN or from attackers in close proximity to the WSN. From the reviewed research, there is limited research available on the effects of DoS attacks (see Chapter 3), targeting the reliability of WSNs that originate from connected networks, such as the Internet.

1.2 DoS Attacks

The objective of a DoS attack is to render a resource inaccessible or degrade a resource for other users (Mirkovic et al. 2004). DoS attacks can take many different forms, a review of which is available in the literature review (Chapter 3).

However in general DoS attacks involve one or more attacking machines, either accessing a service with the intention of overwhelming the victim's resources and preventing other users from gaining access or alternatively an attacker may exploit a known vulnerability in the victim system to disrupt services (Mirkovic et al. 2004). This problem is an order of magnitude greater for resource limited WSNs, where a potential attacker may wield relatively limitless resources against a WSN's limited resources. This asymmetrical situation complicates protecting WSNs from DoS attacks (Perrig et al. 2004). From the literature review (see Chapter 3), there is a substantial amount of literature available on DoS attacks, on large relatively resource rich networks that originate from the same network or from connected networks such as the Internet, and also on DoS attacks on WSNs that originate from the same WSN or from an attacker in close proximity to the WSN. However, as previously stated, there is limited work, which has reviewed the effectiveness or scalability of the existing DoS defence approaches for protecting resource limited WSNs from DoS attacks originating from relatively resource rich connected networks, such as the Internet.

The work in this thesis focuses on the development of an enhanced secure and reliable remote access approach for WSN based HASs. The incorporation of DoS defences is crucial for the provision of reliable communications and is dependent on the remote access approach adopted. Moreover, the connection of WSN based HASs with the Internet results in the security weaknesses in the remote access approaches directly affecting connected networks (Mirkovic et al. 2004), such as WSN based HASs. Consequently, enhancing the security of remote access approaches also enhances the security of connected networks (Kumar et al. 2006), such as WSN based HASs.

1.3 Research Challenge

The research in this thesis investigates the effects of remote DoS attacks on WSN based HASs and the effectiveness of the existing DoS defences for providing WSN based HASs with protection. Protecting WSNs from remote DoS attacks presents a challenge, because WSNs are resource limited and as such do not have sufficient resources available to implement the same security mechanisms as relatively resource rich computers, such as DoS defences (Perrig et al. 2004).

Additionally, the challenge is increased when defending against a remote DoS attack, where there may be multiple, resource rich, attackers targeting a single resource limited WSN (Kumar et al. 2006). Moreover, as identified by (Mirkovic 2003) the most effective DoS defences do not effectively filter out all attack traffic, which poses a problem for resource limited WSNs, where due to their resource limited nature, a low-level DoS attack is sufficient for a DoS attack, as identified and evaluated in Chapter 7.

1.4 Motivation for the Research

As discussed, WSN based HASs offer the potential for a significant improvement in the quality of life for homeowners. Moreover, in the current climate with increasing evidence supporting the case for global warming and increasing fuel bills, WSN based HASs offer the potential for the development of novel energy saving applications. However, for WSN based HASs to be successfully adopted the associated security challenges must be addressed. Additionally, in relation to the provision of secure and reliable remote access to WSN based HASs, there remains a large gap in the knowledge. There is little research available to suggest that existing DoS defences are effective at protecting WSN based HASs.

1.5 Objectives of the Research

The primary research aim, of the research, is to further the work by designing and implementing an improved secure and reliable remote access approach for WSN based HASs, that has an increased resistance to DoS attacks whilst providing an increased level of privacy for the homeowner's personal information.

1.5.1 Objectives

The specific research objectives associated with obtaining the research aim are as follows:

- Investigate the existing literature available on WSN based HASs and the associated methods for remotely accessing WSN based HASs.

- Design and implement a WSN based HAS test-bed that incorporates the common remote access approaches, for evaluating the approaches developed as part of the research.

- Research the current literature available on DoS attacks and Defences for WSNs to obtain a better understanding of the topic.

- Propose and evaluate approaches for enhancing the security and reliability of WSN based HASs, with an emphasis on improving the DoS resistance of WSN based HAS's and the associated remote access approaches.

    - Develop the existing dominant remote access approach "GHS", identified from the literature review (see Chapter 2), on the WSN based HAS test-bed.

    - Develop a model of the most effective DoS defence "D-WARD", identified from the literature review (see Chapter 3) and integrate it with the WSN based HAS test-bed.

    - Develop a DoS attack tool capable of launching an application level DoS flooding attack.

    - Develop and implement a conceptual model of an improved hybrid communications approach for mitigating DoS flooding attacks targeted at the third party mediating communications.

    - Evaluate the effectiveness of the approach, using the existing GHS approach as a benchmark on the WSN based HAS test-bed.

    - Develop and implement a conceptual model of an improved hybrid communication approach for mitigating DoS flooding attacks that directly target WSN based HASs.

    - Evaluate the effectiveness of the approach, using the existing D-WARD approach as a benchmark on the WSN based HAS test-bed.

- Develop and implement a conceptual model of an improved hybrid communication approach for mitigating DoS flooding attacks that target the home gateway.

- Evaluate the effectiveness of the approach, using the existing D-WARD approach as a benchmark on the WSN based HAS test-bed.

1.5.2 Contributions of the Research

The contribution of the research detailed in this thesis consists of five parts. The first contribution is the design of a WSN based HAS test-bed for empirically analysing the existing and proposed approaches. Most of the existing work is theoretical, consequently providing a test-bed to empirically evaluate the existing and proposed approaches, adds to the available knowledge from a different perspective, which takes into consideration environmental variables that cannot be fully represented in theoretical models. Moreover, the test-bed allows for the creation of benchmarks from existing approaches (GHS and D-WARD) to contrast with the proposed approaches (RHS-1, RHS-2, and Hybrid). The quantitative results derived from the evaluation of the proposed approaches on the test-bed are described in the following contributions.

Secondly, this thesis presents the first study to summarise the existing methods for remotely accessing, monitoring, and controlling HASs. Namely, the Direct and GHS communications approach. The approaches have been qualitatively evaluated to highlight the direct access approach is not suitable for monitoring and controlling WSN based HASs, due to the dynamic nature of the IP addresses in the UK, where the IP address of a HAS cannot be known before a direct connection attempt. Moreover, the approaches have been quantitatively evaluated to show that the direct access approach is the fastest of the existing remote access approaches analysed to login, share secure parameters and send three consecutive commands, taking on average 2661ms (a minimum of 2604ms and a maximum of 2793ms). For the same experiments, the GHS approach is shown to be a minimum of 39.23% slower, on average 45.81% slower, and a maximum of 46.60% slower.

The third contribution is the identification of a vulnerability in the communications privacy of remote users communicating with HASs using existing

third party mediated communications approaches, at the third party. The vulnerability allows users at the third party to view homeowner's confidential information, when it is decrypted at the third party for rerouting. Consequently, a secure tunnelling approach for protecting the communications privacy of remote users communicating with WSN based HASs (called the RHS-1 approach) has been designed and implemented. The dual tunnelling method adopted in the RHS-1 approach removes 100% of the confidential information that is visible using the current GHS communications approach.

The fourth contribution is the creation of a hybrid remote access approach for mitigating the effect of DoS attacks targeted at a third party mediating communications between remote users and the WSN based HAS. The hybrid communications approach has been quantitatively analysed in terms of the improvement of DoS resistance compared to the benchmark GHS approach. The results shows that compared to the GHS approach the proposed hybrid approach decreases the time the HAS services are unavailable by a minimum of 58.28%, on average by 59.85%, and a maximum of 61.45%.

The fifth contribution presents an analysis and experimental evaluation of a generic model representing existing DoS defences. The model represents the most effective DoS mitigation tool identified from the domain analysis D-WARD (Removes 99.4% of attack packets). The evaluation shows that this approach is ineffective for protecting resource limited WSN based HASs. The evaluation highlighted that a flooding DoS attack directly targeting a WSN based HAS in a star configuration, at a 256ppm attack rate, results in a sufficient amount of attack data penetrating the existing D-WARD DoS defences to result in an average packet loss rate of 86.25% (a minimum of 84.38% and a maximum of 93.75%). In the partial mesh configuration, the 256ppm attack rate results in an average packet loss rate of 91.25% (a minimum of 85.75% and a maximum of 94.75%). Moreover, a flooding DoS attack targeting the home gateway at 1090 attacks per minute, results in a minimum connection latency of 7130ms, an average latency of 7431ms and a maximum latency of 7942ms. A defence called the "virtual home" is implemented at the edge of the WSN, alongside existing defences, to filter all incoming traffic,

using a cryptographic approach to remove all attack traffic, preventing it from reaching and disrupting the WSN.

The virtual home has been experimentally shown to reduce the percentage packet loss on the WSN during an effective DoS attack. In the case of the WSN based HAS in the star topology, the proposed defence approach has been shown to reduce the percentage packet loss on the WSN, during a flooding DoS attack, by a minimum of 84.70%, with an average reduction of 91.13% and a maximum reduction of 95.6%. In the case of the WSN based HAS in the partial mesh topology, the proposed defence approach has been shown to reduce the percentage packet loss by a minimum of 78.34%, with an average reduction of 91.20% and a maximum reduction of 95.60%.

Additionally, the proposed approach has reduced the average connection latency experienced by remote users connecting to a WSN based HAS during an effective DoS attack against the gateway sensor node in all of the trials conducted. In an experiment with a 799 attacks per minute rate, the proposed approach resulted in a minimum reduction in connection latency of 56.11%, an average reduction of 56.71%, and a maximum reduction of 57.77%. In the experiment with a 2300 attacks per minute rate, the proposed approach resulted in a minimum reduction of connection latency of 90.14%, an average reduction of 90.90%, and a maximum reduction of 91.88%.

All of the contributions aim to create an improved approach for securely and reliably accessing WSN based HASs and consequently enhance the overall security of WSN based HASs.

1.6 Organisation of the Thesis

The structure of this thesis is as follows: Chapter 2 reviews the development of WSN technologies and WSN based HASs. Chapter 3 provides a thorough review on the existing state of research into the field of WSN security, with a special emphasis on existing DoS attacks and counter measures. Chapter 4 defines the research methodology adopted. Chapter 5 introduces the development of a state of the art WSN home automation test-bed, on which the proposed approaches are implemented and evaluated. Chapter 6 introduces an improved approach for the secure remote access of WSNs, focusing on providing improved protection against

attacks targeting third parties involved in the communication process. Additionally an evaluation contrasting the proposed scheme against existing secure remote access approaches is provided. Chapter 7 identifies a new low-level DoS attack against WSN based HASs, and extends the proposed approach introduced in the previous chapter to include protection against DoS attacks focusing on the home end of communications. A new scheme for detecting DoS attacks is proposed, alongside a new mechanism for responding to DoS attacks. Chapter 8 provides the analysis of an evaluation of the proposed approaches conducted through focus group studies, questionnaires and a field trial. Moreover, the chapter introduces the first study to identify the social and ethical issues that arise, from the adoption of WSN based HASs and the associated remote access approaches. Chapter 9 concludes the thesis with a summary of the main contributions of the research as well as areas for future research.

Chapter 2

Wireless Sensor Networks and Home Automation

2.1 Introduction

This chapter provides a comprehensive review of WSNs, with a special emphasis on WSN based HASs. The review is undertaken to partly meet the research objectives set out in Chapter 1. This includes conducting a thorough review of related work to aid in the development of a WSN based HAS test-bed for the subsequent identification and verification of security weaknesses in existing remote access approaches for WSN based HASs and testing of the proposed improved approaches.

2.2 Computer Networks

Computer technology plays an important role in the lives of many people around the world. Computers are present in people's homes, workplaces, and are increasingly present throughout the whole of society. Computerised technology takes many differing forms including, personal computers, aeroplanes, trains, traffic lights, DVD players, and recently clothing comprised of one or more computerised devices.

Over the last decade and in parallel to the advances in computerised technology, communications technology has seen an exponential growth in the consumer market. In 2008, 16 million households, 65% of the population of the United Kingdom had access to the Internet (National Statistics 2008). However, it should be noted that the success of computer and network technology is not independent from one another. The merger of these technologies to form computer networks "a collection of autonomous computers interconnected by a single technology" (Tanenbaum 2003), have encouraged wide spread adoption of these technologies through the development of revolutionary new services that have fundamentally changed the way people live their lives. These services include, email, the World Wide Web (WWW), social networking, blogging, and home automation.

There are a number of different types of computer networks. The most popular types of network include personal area networks (PANs), local area networks (LANs), metropolitan area networks (MANs), wide area networks (WANs), and the Internet. These computer networks differ, primarily in their geographical distribution, see Table 2-1 (Tanenbaum 2003).

Table 2-1: Different types of networks based on geographic distribution

Distance between nodes	Possible location of neighbour nodes	Network type
1 m	Square Metre	Personal area network
10 m	Room	Local area network
100 m	Building	
1 km	Campus	
10 km	City	Metropolitan area network
100 km	Country	Wide area network
1000 km	Continent	
10 000 km	Planet	Internet

2.2.1 Personal Area Networks

PANs are short-range networks, potentially only a few metres in range, which are normally in close proximity to the individuals interacting with them. Moreover, PANs provide relatively low bandwidth communications for either short-term networks created solely for the purposes of performing a single task, such as transferring a picture between connected devices, or longer-term networks for

performing low data rate activities. Examples of recent PAN standards include Bluetooth, ZigBee, IEEE 802.15.4 and Z-Wave.

2.2.2 Local Area Networks

LANs normally operate within a relatively small area (10 to 100m), providing coverage for a single room, building or campus. There are wired and wireless versions of LANs, normally with stable architectures, that can traditionally provide data rates of 10 to 100 Mbps, with newer LANs providing support for up to 1 Gbps. These LANs are conventionally used for sharing resources such as printers, scanners, Internet connections, and network storage servers amongst connected devices.

2.2.3 Metropolitan Area Networks

MANs normally operate over large areas (10km) and provide services for a large number of users, potentially providing citywide access. MANs can be composed of a single large network providing services within the boundaries of a city or be composed of smaller interconnected LANs. However, due to the longer range and larger number of potential users, the data rates received by individual users are less than those offered by LANs.

2.2.4 Wide Area Networks

WANs span a very large area (100km – 1000km), often encompassing a country or even an entire continent. WAN can be private networks, where only users authorised by the network owners have access rights, or public networks, where everyone has access rights.

2.2.5 Global Networks

Global networks span the whole Earth, the most famous global network is the Internet. The Internet is comprised of a complex architecture of interconnected networks, including all of the previously introduced network types. The complexity of the Internet's architecture is further increased because the different types of networks consist of different hardware, software and protocols.

The work in this thesis focuses on WSN based HASs. WSN's are a form of PAN that are becoming more popular for domestic and industrial applications, where people wish to monitor environmental conditions.

2.3 Wireless Sensor Networks

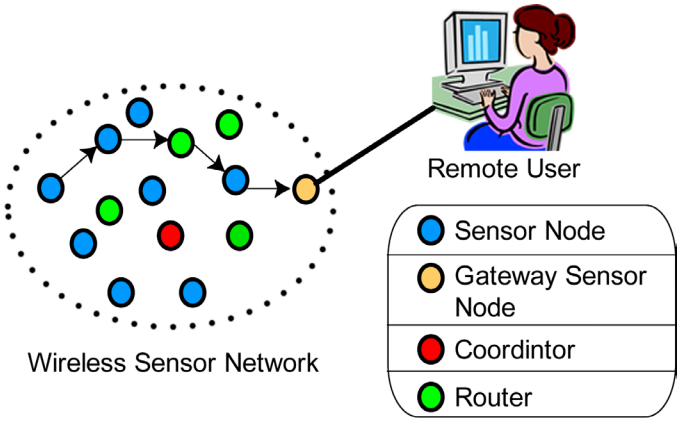

Figure 2-1: A generic WSN architecture

A WSN is composed of low cost, low power, multifunctional sensor nodes that are small in size and communicate wirelessly over short distances (Akyildiz et al. 2002). The sensor nodes collaborate to sense and collate information about their environment, through a set of transducers and a radio receiver (Barontib et al. 2007), and to forward information towards a central sink node. Moreover, information from the sensor node is accessed through a gateway sensor node as depicted in Figure 2-1, which provides a point of ingress between the WSN and either a direct link to a relatively resource rich computer or indirectly through a LAN to a resource rich computer.

There is a greater deal of flexibility when it comes to the deployment choices for WSNs compared to other networks. WSN nodes once distributed randomly in an environment organise themselves into a coherent information sharing network. Consequently, the design time considerations arising from the use of a fixed network structure, do not apply.

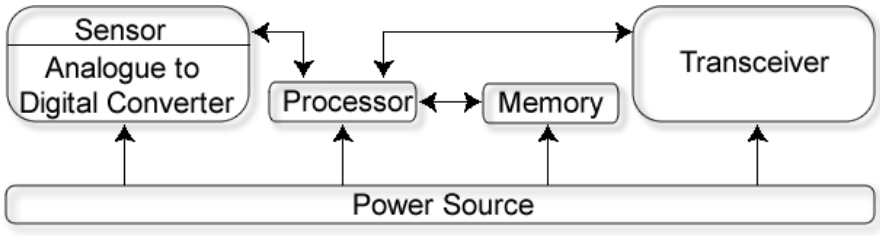

Figure 2-2: The structure of a WSN node

A WSN node, as depicted in Figure 2-2, consists of five main components, a processing unit, memory, transceiver, sensors and power supply. The processor unit is responsible for making the WSN node collaborate with other sensor nodes, and execute application code. The memory unit stores the node's programmes, including the network stack and application programmes. The transceiver allows the node to communicate with neighbouring nodes. The sensor component consists of two parts. Firstly, there is the analogue sensing component that physically measures environmental characteristics such as temperature. Secondly, there is the analogue to digital converter that transforms the analogue environmental readings into a digital representation that can be handled by the nodes processor. One of the most important components of the node is the power supply. The power supply provides the node with life, and is normally limited so that once the node's power supply is exhausted the node can no longer operate. There are other elements that a node may consist of such as power generating components (i.e. solar panels and thermocouples) to recharge the node's power supply , however the five components discussed are crucial for a node to be considers a WSN node, whereas the other components are optional.

2.3.1 Types of Wireless Sensors

A WSN node may consist of one or more sensors. Moreover, there are numerous different types of sensors produced by different manufactures. However, the primary objective of all sensor nodes is to monitor their immediate environment for a wide variety of ambient conditions. A short summary of the ambient conditions monitored by existing nodes that have been identified by (Akyildiz et al. 2002) and (Lewis 2004) follows:

- Temperature,

- humidity,
- vehicular movement,
- lightning conditions,
- pressure,
- soil component levels,
- noise levels,
- the presence or absence of certain kinds of objects,
- mechanical stress levels on attached objects, and
- the current characteristics such as speed, direction, and size of an object.

2.3.2 WSN Stack

The Open Systems Interconnection (OSI) seven-layer model, proposed by the International Organisation for Standardisation (ISO), forms the basis of the design of the WSN protocol stack. However, unlike the seven-layer OSI model that consists of the physical layer, data link layer, network layer, transport layer, session layer, presentation layer and, application layer, the WSN protocol stack does not adopt all seven layers of the OSI model. In reality, the seven-layer OSI model has too many layers making it overly complex and difficult to implement (Aschenbernner 1986). Consequently, the protocol Stack adopted by WSNs consists of five layers, as depicted in Figure 2-3.

The five-layer WSN protocol stack consists of the physical layer, data link layer, network layer, transport layer and the application layer. Each layer is designated a specific set of task to perform independently of the other layers of the protocol stack.

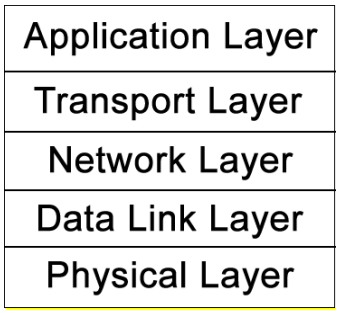

Figure 2-3: WSN protocol stack

The first layer of the protocol stack, the physical layer, is responsible for defining and managing the connections between respective devices and their communication medium. The physical layer is responsible for frequency selection, carrier frequency generation, signal detection, modulation and data encryption. Moreover, the physical layer defines the type of connectors and cables compatible with the communication medium.

The second layer of the protocol stack, the data link layer, is responsible for providing services that allow multiple nodes to successfully access and share a communications medium. These services include medium access control, reliable delivery, error detection and error correction.

The third layer of the protocol stack, the network layer, is responsible for establishing the communications paths between nodes in a network and successfully routing packets along these paths. The objective of different routing protocols and hence the communication paths set up can vary. Some routing protocols will favour communication paths that help the WSN deliver the best Quality of Service (QoS), other energy saving protocols may choose the path that helps the WSN achieve the best lifetime and other will use a hybrid of objectives.

The fourth layer, the transport layer, is responsible for providing higher-level layers of the protocol stack and consequently users with transparent and reliable communications between end users. There are varying forms of transport layer protocols, two of the most popular and contrasting are transmission control protocol (TCP) and user datagram protocol (UDP). Connection oriented transport layer protocols, such as TCP, provide a reliable communication service, with extensive error handling, transmission control, and flow control. Whereas,

connectionless transport layer protocols, such as UDP, provide an unreliable service with the minimum error handling, transmission control, and flow control. In terms of WSNs, TCP/IP is generally not employed directly on WSNs because, as identified during experiments by (Kuorilehto et al. 2006), the flow control mechanisms adopted by TCP is too aggressive for WSNs, where most errors are caused by bit errors and topology changes instead of congestion. Moreover, TCP/IP requires a large processing overhead, which in experiments resulted in five times more power consumption than a WSN specific TDMA-based MAC protocol. There are a number of routing protocols designed specifically for WSNs. For a review of these protocols, please refer to (Akkaya and Younis 2005).

The fifth and final layer, adopted by most WSNs, is the application layer. The application layer resides close to the users of the system. There are many potential applications implemented at the application layer including, Telnet, Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), and Simple Mail Transfer Protocol (SMTP). In terms of WSN's, the application layer programming primarily deals with the processing of sensed information, encryption, formatting and storage of data. Moreover, the application layer examines the underlying layers to detect if sufficient network resources and services are available to meet the user's network requests.

2.3.3 Wireless Sensor Network Standards

A standard is a documented specification, or other precise criteria composed through the collective discussion and agreement by members of a group formed from interested parties such as governments, manufactures, research organisations, consumers, or a selection from some or all of the aforementioned interested parties (British Standards Institution 2009).

Standards allow for the development of products, services or procedures that meet certain minimum levels of quality, safety and performance, whilst providing a greater level of compatibility between devices produced by different manufacturers. Consequently, the compliance with widely known standards provides a certain level of assurance for consumers of the compatibility, and performance to expect from device or services.

Adopting a standard based approach offers a great deal of advantages for both adopters of standards and for consumers. However, there are two primary drawbacks. Firstly, standards normally take a considerable amount of time to be drafted and modified. Consequently, standards do not reflect the latest technology available and require constant and frequent updating to remain competitive. Secondly, standards are a compromised set of specifications agreed upon by different interested parties with different viewpoints. Hence, the standardised approach may not provide the optimal approach. Nonetheless, wireless communication standards have provided consumers with devices that support a vast array of communication technologies for transferring information, such as pictures, electronic documents, sensor readings, between devices.

Recently, the need for low cost, low data rate, battery powered, time sensitive network applications has encouraged further research into the development of Low-Rate Wireless Personal Area Network (LR-WPAN) standards. The most widely researched and adopted wireless standards include Bluetooth, Wi-Fi, Z-Wave, KNX RF, and ZigBee.

Bluetooth is one of the most wide spread LR-WPAN standards in existence. The standard defines a wireless, frequency hopping communication standard capable of forming short-range ad hoc networks. Many devices including mobile phones, headsets, PDA's, laptops, and cars increasingly come equipped with Bluetooth technology for a vast range of applications including transferring pictures, music, files and, GPS data. However, there are two major weaknesses in the Bluetooth standard for use as a LR-WPAN standard of choice. Firstly, Bluetooth technology consumes a considerable amount of energy. Consequently, applications that require real-time monitoring, which require the transceiver to be on for significant periods, need the device's battery to be regularly charged. Moreover, a Bluetooth network or Piconet supports a maximum of one master node and seven slave nodes. Although, Piconets support bridging of co-existing Piconets to form a scatternet. The scalability of Bluetooth is limited for large-scale networks (Salonidis et al. 2005).

The Wi-Fi standard is present in homes and offices across the world and is commonly used for creating LAN's for the connection of devices such as laptops,

printers, and mobile phones. Recently, (Linx 2009) proposed the use of Wi-Fi for creating a PAN in which up to seven devices connect directly, in an ad hoc fashion, with a laptop. Unlike existing Wi-Fi based ad hoc networks the laptop retains the ability to connect and stay connected to a Wi-Fi based LAN. The problems associated with the use of the Wi-Fi standard as a LR-WPAN, as with the problems associated with Bluetooth, include limited connectivity, which reduces the scalability of the standard for large-scale networks. Moreover, the Wi-Fi standard requires a relatively large power supply, which can exhaust the limited power of batteries within a few hours. Consequently, the technology is not, in its current form, appropriate for long term LR-WPAN.

The Z-Wave LR-WPAN standard operates at 908.42 MHz +/- 12kHz in the US and 868.42 MHz +/- 12 kHz in Europe, uses FSK (frequency shift keying) modulation, and supports a data rate of 9.6 Kbps. The standard defines that a Z-Wave network consists of a single network controller, routing-slaves, and slave nodes. The controller maintains information about the network topology and is responsible for autonomously creating and maintaining the Z-Wave network. Routing-slave nodes communicate with predefined destination nodes using routing information downloaded during the initialisation of the routing-slaves. Slaves are at the end of a communication chain and perform actions directly on received messages. Slaves are not capable of routing messages. The standard defines the use of source routing, in which nodes can only communicate with other known nodes. A single Z-Wave network is capable of supporting up to 232 devices, however different Z-Wave networks can be bridged to increase the number of devices supported in a given area. Z-Wave provides a hardware solution for the provision of security features, such as encryption, however the standard does not incorporate a security model. Consequently, security is the responsibility of the system developer. This increases the difficulty of implementing secure LR-WPANs, as developers may not have the necessary security expertise. Moreover, the difficulty of creating compatible systems designed by different manufactures is increased.

The KNX RF is a wireless version of the KNX (Konnex) home and building control standard. KNX RF operates at 868.3 MHz +/- 40-80 kHz using FSK modulation and theoretically supports up to 256 devices. The limited number of

devices supported by the standard may not be sufficient for WSN based automation systems. Moreover, the KNX RF protocol does not support any security functionality as part of the standard, although security features can be adopted by systems programmers at the application layer.

Due to the drawbacks of existing standards such as Bluetooth, Wi-Fi, Z-Wave, and KNK RF as candidates for implementing LR-WPANs, the IEEE (Institute of Electrical and Electronic Engineers) proposed IEEE 802.15.4 as a new LR-WPAN standard. The IEEE 802.15.4 standard is explicitly designed for LR-WPANs such as WSNs and aims to overcome the aforementioned problems associated with the existing standards. Subsequent evaluation of the IEEE 802.15.4 standard after its initial release has identified areas where improvements could be made such as ease of network configuration, need for application programs, and a need for advanced security features. Consequently, the ZigBee Alliance was formed from a consortium of semiconductor manufactures and technology provider from around the world. The IEEE 802.15.4 standard provides the basis of the new standard defining the Physical (PHY) and Medium Access Control (MAC) layers. The ZigBee standard complements the IEEE 802.15.4 standard and provides the Network (NWK) layer, and the Application layer (APL). The IEEE 802.15.4 layers and ZigBee layers combine to form the full layers, see Figure 2-4, of a low cost, low power, and low data rate WSN standard.

2.3.4 IEEE 802.15.4

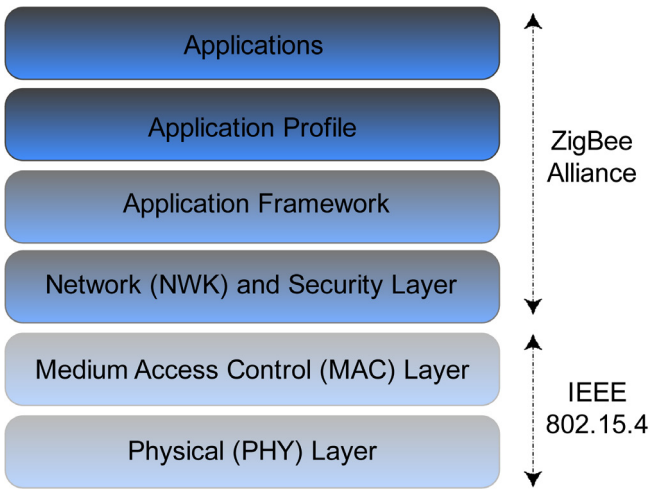

Figure 2-4: IEEE 802.15.4 and ZigBee stack

The IEEE 802.15.4 standard supports the star and peer-to-peer network topologies, as depicted in Figure 2-5. Moreover, the IEEE 802.15.4 standard supports a 64-bit long address and a 16-bit short address, theoretically resulting in a single network being able to support a maximum of $2^{16} \approx 65{,}000$ devices.

As previously discussed, the IEEE 802.15.4 standard defines the PHY and MAC layers for LR-WPANs. The PHY layer is responsible for characterising the physical attributes and behaviours of LR-WPAN nodes. This includes turning the

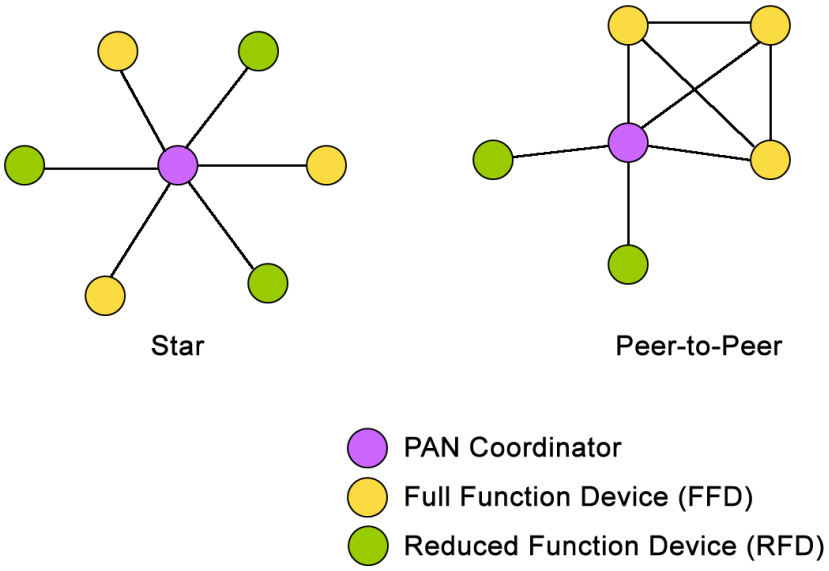

Figure 2-5: IEEE 802.15.4 topologies

transceiver on and off, selecting the appropriate channel, estimating the link quality (LQI), receiver energy detection, and clear channel assessment (CCA) (Barontib et al. 2007). Moreover, the PHY layer supports three licence free ISM (Industrial, Scientific, and Medical) frequency bands including 2.4 GHz with 16 channels and a 250 kbps data rate, 902 to 928 MHz with 10 channels and a 40 kbps data rate and, 868 to 870 MHz with 1 channel and a 20 kbps data rate (Craig 2005 and Ergen 2004).

The MAC layer defines the network structure of LR-WPANs. The IEEE 802.15.4 standard defines two types of devices, full function devices (FFDs), and reduced function devices (RFDs), that can constitute a compliant LR-WPAN. FFD incorporate all the MAC layer functions, including the ability to connect to any node in range and forward messages. This means that a FFD can act as a network

coordinator or a common node. Moreover, FFDs acting as the network coordinator send network beacons providing synchronisation, communication, and network join services. However, it should be noted that due to a lack of a NWK layer, only the coordinator forwards messages. The other common node FFDs can only communicate with their one-hop neighbours. On the other hand, RFDs have access to a limited range of MAC layer functions. RFDs are equipped with sensor and actuators such as temperature sensors and light switches respectively for monitoring their respective environments. Once the RFD is ready to transmit sensed information, the RFD may only communicate with one FFD (Barontib et al. 2007).

The IEEE 802.15.4 MAC layer supports super-frame and non super-frame communications. In super-frame communications, the network coordinator emits a synchronising beacon to indicate the start of a super-frame and a beacon to indicate the end of the super-frame. The super-frame is divided into active times and inactive times where network nodes sleep to conserve energy. The active period is further divided into contention access period (CAP) and contention free period (CFP). During the CAP, nodes compete for access to the communication channel using the Carrier Sense Multiple Access with Collision Avoidance (CSMA-CA) protocol. During the CFP the network coordinator splits the available CFP into guaranteed time slots (GTS) and assigns each slot to a particular device to communicate without contention from any other device on the network. Alternatively, in the non super-frame based approach all devices on the LR-WPAN compete for access to the channel using CSMA-CA. In this case, all devices have an equal chance of gaining access to the channel or not gaining access.

2.3.5 ZigBee

The ZigBee standard is implemented on top of the IEEE 802.15.4 PHY and MAC layers. The objective of the addition is to standardise the upper layers of the protocol stack, through the addition of the NWK and APL layers. As depicted in Figure 2-6, the APL layer consists of the Application framework for distributed application development and communication, the ZigBee device object (ZDO), and the application support sublayer (APS) (Barontib et al. 2007).The application framework can consist of up to 240 “application objects” (APO), user defined modules that comprise the ZigBee application. The ZDO provides services to the

APO, allowing them to discover each other and organise themselves into a distributed application. The APS provides a user-friendly interface for the APS and ZDO to access underlying data and security services provided by the lower levels of the protocol stack.

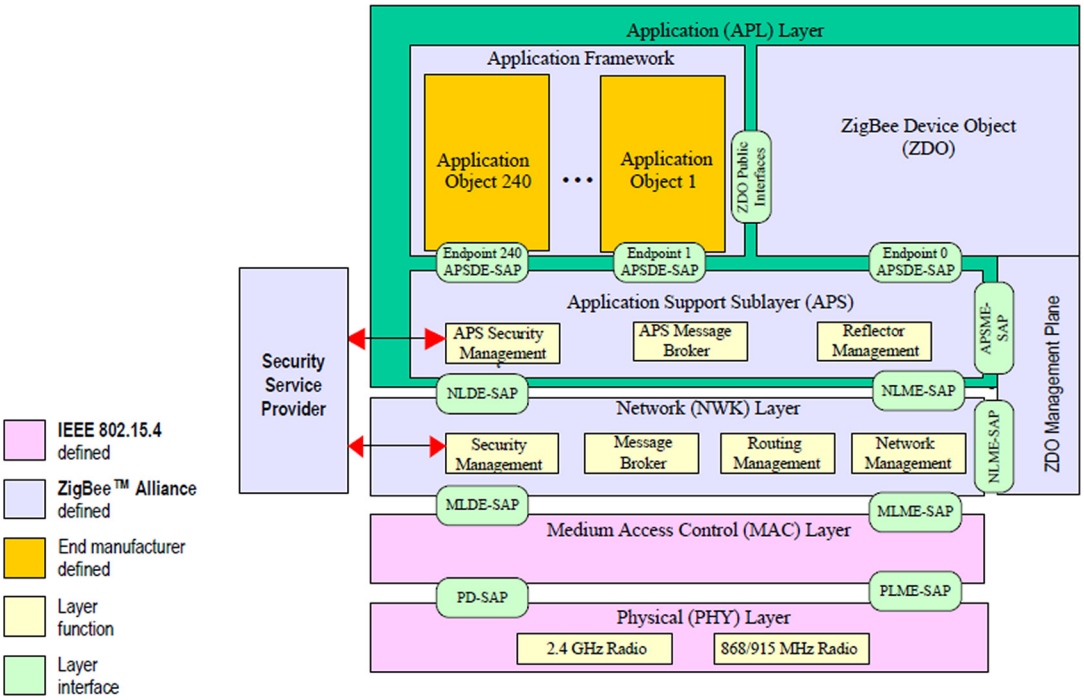

Figure 2-6: ZigBee stack architecture (ZigBee Alliance 2007)

The NWK layer defines three device types, end device, router, and coordinator, that map on to the FFD and RFD specified by the IEEE 802.15.4 standard. Firstly, ZigBee end devices are RFD or FFD providing simple functions. Secondly, ZigBee routers are FFD with routing capabilities and thirdly, ZigBee coordinators are FFD responsible for managing the whole network. The NWK layer supports the underlying topologies discussed earlier, however through the introduction of router nodes provides multi-hop communications. Consequently, more complex topologies such as tree and mesh topologies are supported as depicted in Figure 2-7. Additionally, the NWK layer provides services for route discovery, security, and management of nodes joining and leaving the network.

The ZigBee standard defines a comprehensive security policy. ZigBee assumes an open trust model (Barontib et al. 2007), whereby all the layers, of the protocol stack, are trusted. Consequently, the ZigBee stack distributes the implementation of security across different layers of the stack including the MAC,

NWK, and APS layers, as depicted in Figure 2-6. The basic security primitives defined by the ZigBee stack include:

- ***Freshness***: each ZigBee device records a history of incoming and outgoing freshness counters against which the counters of received messages are checked.

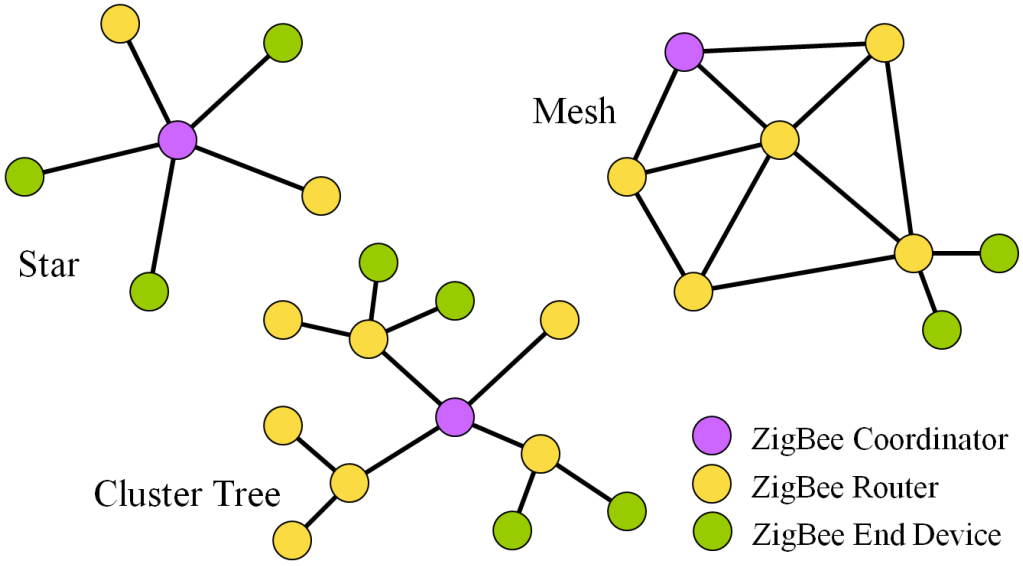

Figure 2-7: ZigBee topologies

- ***Message Integrity***: the standard provides a default level of 64-bit data integrity, and provides 0, 32, and 128 bit data integrity as optional choices.

- ***Authentication***: ZigBee provides network and device level authentication. Network level authentication requires significantly less resources with a single network key used to authenticate all devices. Device or link level authentication requires a unique key for each connection authenticated.

- ***Encryption***: ZigBee provides network level encryption and device or link level encryption. Network level encryption requires one global encryption key, whereas link level encryption requires a unique key for each device or link.

2.3.6 WSN Applications

There is a range of diverse applications that lend themselves to WSNs. (Akyildiz et al. 2002) categorises these under five-application areas, military, environment, health, home and other commercial areas.

WSNs are suitable for use in many military applications including command and control applications, surveillance and reconnaissance of enemy targets, monitoring for the release of biological and chemical weapons and tracking of ordinance. The ability of WSN nodes to be quickly deployed, organise themselves autonomously into functional, fault tolerant networks makes WSN technology ideal for these and many other military applications.

Environmental applications of WSNs include monitoring the movement of wildlife such as birds and insects, monitoring factors that affect the growth of crops, exploring inhospitable parts of the earth that remain unexplored, detecting and tracking forest fires, detecting and monitoring the progress of floods, and measuring levels of pollution across distributed locations.

One of the most promising applications of WSNs for the elderly and infirm is health care. WSNs provide the potential to offer these vulnerable groups a greater level of independence in their lives. Potential applications include integrated control of household devices from a single controller, remote patient monitoring, better real-time monitoring of patients in hospitals and tracking staff and equipment in hospitals.

Home automation technology has been the subject of research for many years. However, largely due to the expense and intrusiveness of installation of these systems, they have failed to achieve wide scale consumer adoption. However, with the low cost, small size, non-intrusiveness of installation, characteristics of WSNs, many of the cost and installation problems identified with existing systems are overcome. The potential applications for home automation technology are diverse, such as multi-media entertainment, automatic houseplant watering, domestic robots, home security, energy saving, and automated pet feeding.

The work in this thesis focuses on the challenges facing the application of WSNs for home automation. The next section explores the existing literature on home automation and the research challenges facing the development of WSN based HASs.

2.4 Home Automation and WSNs

There are many definitions of home automation available in the literature. (Bromley et al. 2003) describes home automation as the introduction of technology within the home to enhance the quality of life of its occupants, through the provision of different services such as telehealth, multimedia entertainment and energy conservation. The existing research into home automation can be categorised based on the communication and networking technology used to create the HAS.

Early HASs relied on the wired medium for networking and communication. The X10 industry standard, developed in 1975 for communication between electronic devices, is the oldest standard identified from this review, providing limited control over household devices through the home's power lines.

HASs based on the wired medium provide reliable and secure systems. However, the use of the wired medium for the formation of networks to facilitate communications between connected devices requires extensive rewiring incurring an intrusive installation and increased installation cost. Additionally, the use of the wired medium limits the positioning of devices to locations close to the physical wired medium (Reinisch et al. 2007). Consequently, recent research into the home automation domain has shifted towards systems incorporating LR-WPAN technology, in particular WSN based HASs are currently the focus of research in the home automation field. The incorporation of WSN technology allows for the creation of smart HASs that monitor and respond to environmental phenomenon. The existing research into WSN based HASs can be categorised based on the WSN standard used to create the HAS.

The Bluetooth standard has been investigated for creating a WSN based HAS. (Sriskanthan et al. 2002) introduced a Bluetooth based HAS, consisting of a primary controller and a number of Bluetooth sub-controllers. In the proposed system, each home device physically connects to a local Bluetooth sub-controller. The home devices communicate with their respective sub-controller using wired communications. From the sub-controller all communications are sent to the primary controller using wireless communications. As discussed earlier, the system suffers from drawbacks attributable to the use of Bluetooth. Furthermore, it is

desirable for each home device to have a dedicated Bluetooth module. However, due to the fiscal expense of Bluetooth technology, a single module is shared amongst several devices. Consequently, devices have to wait for other devices to finish using the Bluetooth module before they can access the module and transmit messages. This has the disadvantage of incurring an additional access delay.

The WSN standard to receive the most attention, for the purposes of home automation and for other LR-WPAN applications is the IEEE 802.15.4 standard. Numerous HASs facilitate the IEEE 802.15.4 standard for the implementation of communication and networking including (Reinisch et al. 2007), (Bolzani et al. 2006), (Gauger et al. 2008), and (Baker et al. 2007). A summary of the recent investigations of the IEEE 802.15.4 standard as a suitable communication protocol for creating a HAS follows:

Certain approaches have integrated the IEEE 802.15.4 standard with existing home automation standards. This facilitates the use of IEEE 802.15.4 features to overcome weaknesses in existing protocols, whilst maintaining the strengths of well known and trusted home automation standards. For example, (Reinisch et al. 2007) proposes the extension of an established wired home automation protocol KNX/EIB (Konnex/European Installation Bus) to the LR-WPAN domain through the integration of the standard with IEEE 802.15.4 to form KNX RF (Konnex Radio Frequency). The combination of the two standards provides security features available in the IEEE 802.15.4 standard, whilst adding the potential for future compatibility with the ZigBee standard.

Other approaches have relied solely on IEEE 802.15.4 as the basis of the HAS, including (Bolzani et al. 2006), (Gauger et al. 2008), and (Baker et al. 2007). (Bolzani et al. 2006) evaluated the ability of IEEE 802.15.4 to provide real-time environmental information for home automation applications. This research project has implemented an IEEE 802.15.4 based sensor network and integrated it with a simulator of a HAS called “Home Sapiens”. The simulator generates normal user behaviour and requests functions from the integrated IEEE 802.15.4 network. The evaluation tested the ability of an IEEE 802.15.4 based HAS to respond to normal user activities. The evaluation concluded that IEEE 802.15.4 sufficiently dealt with the demands placed on the network from simulated activity without incurring

abnormal behaviour such as excessive communication delays or incorrect operations on the home automation network.

(Baker et al. 2007) conducted one of the most comprehensive studies into the potential home health care applications for the IEEE 802.15.4 standard. Five home health applications based on IEEE 802.15.4 WSN technology, were developed including:

- "Sleep safe" a sensor to alert parents when their baby roles over onto its stomach, increasing the risk of sudden infant death syndrome (SIDS).
- "Baby glove" a blanket for premature babies that has sensors to measure the baby's temperature and hydration level more accurately and economically than existing approaches.
- "Fireline" a shirt embedded with sensors to monitor the heart rate of fire fighters and raise an alarm when their heart rate becomes abnormal.
- "Heart@home" integrated WSN technology with an existing blood pressure monitor to send and store sensed information to a local PC.
- "LISTEN" located a sound sensor close to devices, such as doorbells, and other noise making devices, when the sensor detected sound a visual alarm was triggered. Alerting deaf or hearing impaired users of household devices that require attention.

As discussed, the IEEE 802.15.4 standard offers a low cost, battery powered, solution for networked applications. However, the standard does not provide an approach for different manufactures to produce compatible home automation devices. Moreover, the complexity of creating compatible devices is increased, as there is no common network layer, resulting in IEEE 802.15.4 home automation devices incorporating varying routing protocols and network topologies (Barontib et al. 2007). Consequently, ZigBee based HASs have emerged to tackle the shortcomings of IEEE 802.15.4 based HASs, including (Varchola et al. 2007), (Wu et al. 2008), (Sun et al. 2008), (Collotta et al. 2009), (Jin et al. 2008), and (Virone et al. 2006). ZigBee builds upon IEEE 802.15.4 to increase the ease of

deployment, and scalability of the home automation network whilst providing reconfiguration and self-organisation abilities for home automation devices. Most ZigBee based HASs identified have focused on a single application, for example (Sun et al. 2008) shows the development of a ZigBee based lighting system, and (Collotta et al. 2009) develops a central heating control system using multiple distributed temperature sensors to more accurately control heating levels within the home. There is limited literature available on research investigating the appropriateness of ZigBee for use with a complete HAS. However, (Wu et al. 2008) has attempted to address this gap in the literature through the development of a ZigBee based "Intelligent Home System" consisting of a Home Server, GSM Module, intelligent home appliances, and environment detection sensors. The HAS adopts a one-hop, star topology, with all sensors and appliances connected directly with the home server. The home server is the network coordinator and all other devices are end devices. The system is integrated with commercially available temperature, humidity, luminance, vibration and security sensors. The home server waits for an alert from the connected devices and sensors. Once an alert is received, the GSM module sends a text message to the respective homeowners, informing them of the alarm. In turn, a homeowner may send a text to the GSM module containing instruction, which the home server interprets and consequently modifies the respective home automation device.

The existing HASs, developed as part of academic and industrial research, have normally provided remote access for the monitoring and control of household devices. Remote access involves creating a bridge between HASs and neighbouring networks with a greater geographic range, such as LANs, MANs, WANs, or global networks. In many WSN applications, where WSNs are deployed to measure extreme environments in remote locations, such as monitoring volcanoes, remote control is a critical component of the WSN infrastructure, allowing inhospitable environments to be monitored from a safe distance and at leisure. In the case of WSN based HASs, many of the applications, such as telehealth, which utilise the expertise of specialist individuals or organisations, incorporate remote access as a critical component of the WSN infrastructure. The following section reviews a summary of the most popular, existing remote access approaches.

2.5 Remote Access Approaches

The earliest remote access approach, identified by the authors review, was proposed by (Corcoran et al. 1996). A method for remotely accessing a CEBus home automation network, using the WWW was proposed. The system proposes the use of a direct connection from the remote access device to the HAS. The user loads a webpage using a HTML browser, stored on the home's web server. An applet is loaded by the html page, which initiates a TCP/IP (Transmission Control Protocol/Internet Protocol) connection with the home's web server. All incoming messages are routed, by the web server, to the CEBus network. This system shows an early example of remote access with no security implemented. However, this approach outlines the fundamental framework used for remote access by most systems today.

More recent "secure remote access approaches" fall into two general categories. Firstly, there are those, like the aforementioned system, that connect remote devices directly with the destination system. Secondly, there are those that use a third party to mediate the connection between the remote device and the destination system.

(Duncan et al. 2000) proposes and implements a scheme for direct remote access. The system comprises of a medical data repository in a hospital which remote users can access using a handheld PDA. A dedicated domain name is assigned to the hospitals static IP address. Remote users connect to the repositories domain name using a PDA and by submitting a username and password. The connection is protected using a combination of SSL (Secure Socket Layer) and elliptic curve cryptography. Moreover, the repository is located within a decentralised zone, where a firewall filters the types of connections allowed from public networks. In the eventuality of a breach in security, the system automatically generates an analysis of the system usage, allowing any unauthorised access to be detected.

(Hu et al. 2007) propose creating a virtual private network (VPN) between authorised entities. The connections between the communicating entities, that form the VPN, are created by establishing SSL tunnels between them. Once these

connections have been established messages flow, through these tunnels, between entities as if they were connected on the same network.

There are many other direct access approaches; however, the underlying approach used for direct access approaches is the same. In terms of accessing WSN based HASs using direct access approaches, there are several problems. Firstly, most homes in the UK do not have a static IP address. Consequently, there is no method for the remote user to know the IP address of their respective home or WSN based HASs. Moreover, the use of a static IP address provides a fixed point for attackers to launch a prolonged attack. In Addition, the direct access approaches place the emphasis of maintaining security on the owners of the HAS. For example if the earlier discussed system proposed by (Duncan et al. 2000) is adopted for HASs, the users need extensive security knowledge on the use and maintenance of SSL certificates, and firewalls. Consequently, the use of a direct access approach for WSN based HASs may not be possible or appropriate.

Recently third party based approaches for providing remote access have been suggested to overcome the problems identified with direct access approaches for WSN based HASs. (Bergstrom et al. 2001) proposed a scheme in which a server located in the home environment establishes a connection with a trusted third party, called a Global Home Server (GHS) and supplies it with its current IP address. The remote user connects to the GHS, and sends it encrypted messages. The GHS decrypts the messages and looks up the messages destination in the database of connected homes. The GHS re-encrypts the information and forwards the message to the appropriate home's IP address. In parallel (Kara 2001), and later (Kara 2004) proposed an almost identical scheme. In this scheme the mobile client's first message to the trusted third party contains security information required by the HAS to establish end-to-end security. This information is passed to connecting remote entities by the trusted third party. The remote entity and HAS use this information to establish end-to-end security and encrypt all communications. The third party based approaches differ from direct access approaches primarily due to the direction of communication connections. Direct connections are initiated by a client and are received by a HAS as incoming connections. Whereas, in third party based approaches the HAS initiates an outgoing connections to a third party and waits for

data from a client on the outgoing connection, routed through the third party. Although the third party based approaches have been shown to provide effective remote access for HAS, no comparative analysis evaluating the differences and compromises between using direct and third party based remote access approaches for accessing WSN based HASs is available. Moreover, from this review no research is available, which analyses the security of these approaches.

2.6 Conclusions

This chapter has provided an overview of the development of WSN technology. Moreover, an overview highlighting the development of HASs from wired to WSN based HASs is presented. The earliest wired HAS identified from this review is presented, showing the weaknesses identified by subsequent research including the intrusive, costly installations of wired HASs and the incompatibility of systems designed by different manufactures. Wireless networks and in particular WSNs based on standards are shown to overcome many of the problems associated with the earlier wired HASs.

Figure 2.2: Technical analysis of Wireless Standards

Wireless Standard	Power Usage	Maximum Devices	Data Rate	Manufacturer Interoperability	Security
Bluetooth	High	8	1,3 Mb/Sec	Profiles	Pass code
Wi-Fi	High	8	54, 600Mb/Sec	Profiles	WPA/WPA2
Z-WAVE	Low	256	9.6 Kbps	Non	AES
KNX-RF	Low	256	16.384 Kbps	Non	Non
IEEE 802.15.4	Low	65000	20, 40, 256Kbps	Non	AES
ZigBee	Low	65000	20, 40, 256Kbps	Profiles	AES

Table 2.2 provides a technical summary of the different wireless standards investigated in this chapter. The ZigBee standard due to its low power consumption, support for up to 65000 devices, use of a well established security mechanism (the advanced security standard, discussed further in Chapter 3), and support for device profiles is considered the most suitable standard for the creation of WSN based HASs. Where, Bluetooth and Wi-Fi's reliance on a relatively high power supply makes them unsuitable for battery-powered devices. Additionally, the low data rate of both Z-WAVE (9.6Kbps) and KNX-RF (16.384Kbps) and lack of support for the creation of compatible products from different manufactures, supports the

appropriateness of ZigBee as the most suitable WSN based HAS standard. Moreover, for the same reasons, the lack of manufacture interoperability offered by IEEE 802.15.4 also supports the use of ZigBee as a WSN based HAS standard.

In addition, the remote access approaches used commonly to access HASs are categorised based on the approaches, which form direct connections and those, which use third parties to mediate connections. The direct access approaches are shown to have an inability to directly connect to HASs in the UK due to the common use of dynamic IP addresses, resulting in direct access approaches not having the required IP address to successfully establish a connection. Moreover, the direct access approaches are shown to place the emphasis on maintaining security on the homeowners, although they may not have the required expertise.

Third party based remote access approaches are shown to overcome the dynamic IP address problem. However, there is a lack of quantitative analysis of the comparative performance of the direct and third party based GHS remote access approaches. Furthermore, most research on remote access approaches focuses on the formation of communication links and ignores security concerns such as the resilience to DoS flooding attacks of direct and third party based approaches.

The existing security threats faced by WSN based HASs and the respective remote access approaches are reviewed in Chapter 3. Moreover, the following chapters introduce a WSN based HAS test-bed, designed based on the literature review, which is used to provide a quantitative performance analysis of the existing direct and GHS remote access approaches, a benchmark based on the GHS approach and the evaluation of proposed approaches based on the GHS benchmark. Please see Chapter 6 for the results of the Quantitative analysis.

Chapter 3

DoS Attacks in WSNs

3.1 Security Overview

Computer security is a relatively recent development. In the time before computers data was kept locked in filing cabinets. When computers were developed a strategy was required to keep data on these computers safe, this was termed Computer Security. Due to the advent of distributed systems connected by networks across the internet, there arose a need to keep data safe between these networks, this was termed Internet Security (Stallings 2002).

Standards have emerged to help system designers develop systems that offer a comprehensive range of security services, in an attempt to provide an acceptable level of security for adopters of the standards. A widely accepted standard is the ITU-T (International Telecommunications Union Standardisation Sector) defined X.800 standard. The standard provides a security architecture for the OSI Model, defining security requirements and suggesting approaches for satisfying these requirements. There are, as identified by the X.800 recommendation and argued by (Stallings 2002), security categories which must be satisfied in order to classify a system as secure, these categories include authentication, access control, confidentiality, data integrity, non-repudiation, availability, and fairness.

3.1.1 Authentication

The authentication process is concerned with the verification of the identity of an entity (peer authentication) or the verification of the source of a received message (data authentication). In peer authentication, the identity of an entity is confirmed in order to gain physical access to a building or electronic access to a service. The traditional form of peer entity authentication is password authentication. This form of authentication is commonplace across society from traditional systems employing username and password combinations to authenticate users before providing them with services such as logging into an email account, or signing into an ISP. Through to modern day alternatives, including chip and pin for credit cards to access epos (electronic point of sale) services, or swipe card systems to gain physical access to buildings. Recently, the use of smart cards (Hwang et al. 2000), (Sun 2000), (Shen et al. 2003), (Ku et al. 2004), and biometric data (Khurram et al. 2007) to provide a more secure method for authentication, than passwords, have been proposed. In data authentication the data received is validated to make sure the data was sent from the entity claimed. The objective of data authentication is to prevent third parties from inserting data into pre-existing communications with authenticated entities. Data authentication is a continuous process carried out throughout an authenticated communication. The most common approach for providing data authentication is to use a secret key, only known by the sender and receiver, to encrypt data. The recipient of the data checks the received data has been encrypted with the correct secret key, only if the data has been encrypted with the correct secret key is the data considered authentic.

3.1.2 Access Control

There is a certain degree of overlap between access control and the previously discussed authentication. However, authentication is concerned solely with the verification of an entities identity. Access control, involves the assignment of different levels of access to entities once they have been authenticated. The advantage of assigning different access levels is that the damage a legitimate entity or a malicious entity, using stolen access details, can do to a system is reduced. The disadvantage of this approach is the added complexity to the system design.

3.1.3 Confidentiality

Confidentiality is concerned with keeping data secret from third parties not authorised to view the contents of communications. A system, which implements confidentiality, must protect data from direct and indirect interpretation by unauthorised entities. Direct interpretation involves unauthorised entities intercepting and viewing data. Indirect interpretation involves unauthorised entities viewing communications traffic patterns and deriving the contents of the communications, through traffic analysis.

The primary approach for providing confidentiality is through the use of encryption. There are two categories of encryption used to provide confidentiality, symmetric key cryptography and public key cryptography. The oldest form of encryption is symmetric key cryptography. A function f(x) is shared amongst authorised participants and is used for both encryption and decryption of data. This type of encryption is very fast and is securer than other methods, however requires a secure communication channel for keys to be distributed. Examples of symmetric key cryptography are Caesar cipher, Hill Cipher, One time pad, DES (Digital Encryption Standard) and AES (Advanced Encryption Standard).

The alternative approach to symmetric key-based confidentiality is known as public key cryptography (PKC). In this approach, there are two keys, a public key and a private key. The public key is used to encrypt data and the private key to decrypt data. The advantages of public key cryptography over alternative approaches include not having to disclose private keys to any participants and not requiring a secure channel for key distribution.

3.1.4 Integrity

Data integrity is concerned with preventing the unauthorised modification of data, without detection by a legitimate user. There are three established approaches for verifying that a message has not been tampered with, message encryption, message authentication codes, and hash functions.

Message Encryption: The message encryption approach to data integrity, works by creating a message structure and amending a checksum to the message.

The output is encrypted with a secret key. This verifies that only the person with the secret key could have created the message. When decrypted if the message is not in the correct format or the checksum is incorrect, it is surmised the message has been tampered with.

Message Authentication Code (MAC): The MAC is a non-reversible hash code, which computes a smaller output than the source message, using a publicly available function and a secret key. The sender generates the MAC code and sends it with the encrypted data. The receiver regenerates the MAC code using a pre-shared key. If the MAC codes do not match, then it is surmised the message has been modified. The problem with this approach, is that two secret keys are required, one for the encryption and one for the MAC function.

Hash functions: A hash function is similar to a MAC code however does not require a secret key. It relies on the fact that it is difficult to find another message that will produce the same hash quickly. There are two strengths of hash functions. Firstly, there are strong collision resistant hash functions, where it is infeasible to find the same output for two different inputs. Secondly, weak collision resistant functions, where it is infeasible to find a second input that will produce the same hash output when the first input is known.

3.1.5 Non-repudiation

Non-repudiation is the method employed to prove that an entity sent a message and that the recipient entity in the communication received the message. There are two primary approaches used to provide non-repudiation services, digital signatures, and notarization.

When using digital signatures the communications participant sending the message signs the message with a secret key. If the recipient can decrypt the message using the sender's public key, it is implied that the sender is in possession of the corresponding private key so must have sent the message.

In notarization, a trusted independent third party verifies that entities have sent and received messages. The third party keeps records of messages sent and received, so providing Non-repudiation services to the interested parties.

3.1.6 Service Availability

The E.800 recommendation of the ITU-T defines availability as the "ability of an item to be in a state to perform a required function at a given instant of time or at any instant of time within a given time interval, assuming that the external resources, if required, are provided" as defined by (Grottke et al. 2008). In the security domain, service availability research focuses on the protection of service providing systems from attackers that attempt to overwhelm the resources of these systems in an attempt to either permanently remove the service from availability, or to sufficiently degrade a service intermittently removing it from availability. There are numerous methods employed by malicious users to adversely affect the availability of services. However, the methods utilised to adversely affect the availability of services are collectively termed DoS attacks.

The research outlined in this thesis focuses on the improved protection of systems resources, and service availability of WSN based HASs and the respective remote communications infrastructure from DoS attacks originating remotely from other networks. The following section provides a detailed review of known DoS attacks and the existing defence approaches.

3.2 Denial of Service Attacks

A DoS attack is an attempt by an attacker to render a service completely inaccessible or significantly degrade the level of service availability experienced by legitimate users of the service (Mirkovic et al. 2004). Distributed Denial of Service (DDoS) attacks have the same objective as DoS attacks. However, DDoS attacks are carried out from a number of attacking hosts, whereas DoS attacks are carried out from a single host. In this thesis, the term DoS is used to refer to both DoS and DDoS attacks. This chapter and thesis focus on DoS attacks in the realm of computers. In particular, DoS attacks that threaten the availability of WSN based HAS services for local and remote users.

3.2.1 Goals of a DoS Attack

The goal of launching a DoS attack is to inflict damage on a victim. However, there are normally underlying factors behind the desire to inflict damage

on a victim including personal, material, and political factors. In summary, personal factors may include a desire for revenge against the victim from such sources as, disgruntled employees, or a gain in prestige from hackers in the attacker's social network (Mirkovic et al. 2004). An attacker may wish to make a financial gain from the extortion of money from individuals or organisations in exchange for stopping or not instigating an attack against their services. The first recorded large-scale DoS attack conducted over the public Internet occurred in August 1999 on a local network at the University of Minnesota. The attack originated from 227 zombies and resulted in the shutdown of the network for two days (Garber 2000). In terms of political attacks, during a period of war or civil unrest a government may launch DoS attacks on the resource infrastructure of other nations or organisations. An example of such an attack is during the 2009 civil unrest in Iran, the government attempted to block incoming satellite transmissions of media organisations, which were blamed for encouraging the unrest, by jamming the communication frequencies employed by the respective media organisations satellites (Horrocks 2009). Additionally, (BBC 2009) reported on a new wave of DoS attacks targeted against leading South Korean organisations, including the country's largest bank, national newspaper, and spy agency. It was largely reported at the time, that these attacks were politically motivated.

3.2.2 Stages of a DoS Attack

A DoS attack generally consists of four stages, three of which occur before the actual attack takes place. Firstly, to avoid detection, attackers tend not to use their own computers to launch an attack, preferring instead to search the Internet looking for machines with security vulnerabilities that will allow the attacker to subvert them.

Secondly, an attacker hacks into the machines identified during the previous stage and infects them with malicious code. The malicious code contains the attack code, a backdoor to allow the attacker easier access to the infected machine in the future, and code to search for and infect other vulnerable machines. The infected machines are called "Zombies" reflecting the fact the owners of the machines may not be aware their machines are infected. There are many approaches for infecting vulnerable machines including, directly hacking into vulnerable machines, using

automated methods such as sending email with attachments containing the attack code, and using Trojans (legitimate applications containing attack code). A detailed review of the methods available to attackers for infecting vulnerable machines is outside the scope of this thesis, consequently for more information please refer to (Mirkovic 2003). During the third and optional stage, infected machines search for and infect other vulnerable machines.

The fourth and final stage involves the initiation of zombies to start a DoS attack against a victim. The method for initiating an attack may include pre-programming the attack date, time and victim in the attack code or intelligent methods may deliver this information to the Zombies after infection. The second approach has the advantage that the same Zombies can be reused and leveraged against more than one victim. A detailed review of methods for initiating Zombies and starting an attack is outside the scope of this thesis, consequently, for more information please refer to (Mirkovic 2003).

3.2.3 Types of DoS Attack

There are numerous methods for achieving the objective of DoS attacks. However, there are two categories of DoS attack, “Brute Force” attacks and “Vulnerability” attacks. (Mirkovic 2003). Firstly, brute force DoS attacks attempt to overload a network with excessive data in an attempt to overload a network service or connection. Secondly, “Vulnerability” DoS attacks exploit vulnerabilities in a systems hardware or software in order to overload a network service or connection with disruptive data that causes the connection or service to fail. Brute force attacks are harder to prevent because the scale of an attack, in terms of incoming bandwidth, may be significantly higher than for a vulnerability attack. Additionally, it is harder to trace all of the attacking hosts and deal with a sufficient number of attacking hosts in order to stop a brute force DoS attack. Conversely, a vulnerability attack exploiting a weakness in a system may be undertaken from a single host. However, vulnerability attacks can be easily fixed through a software patch or hardware update, once the weakness has been identified.

3.2.4 Source of DoS Attacks

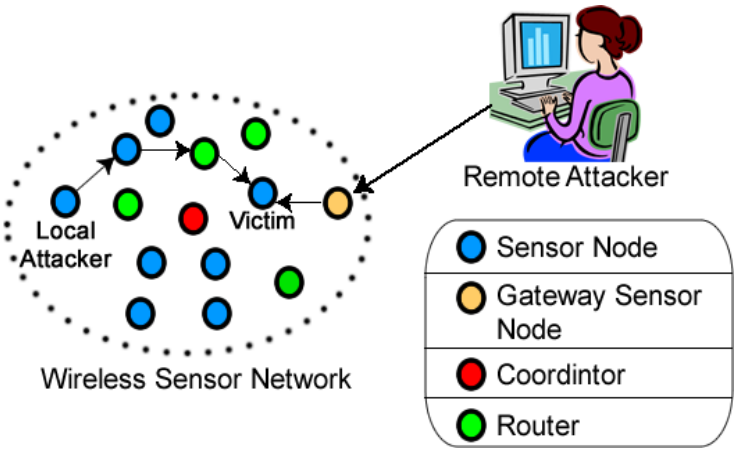

Figure 3-1: Local and remote DoS attacks against a WSN node

As depicted in Figure 3-1, DoS attacks can be categorised based on the source of the attack. Remote DoS attacks originate from outside the network under attack, normally from other publically accessible networks. The Internet is the most widely employed public access network, virtually providing worldwide coverage, adopted by individuals and organisations to interconnect their respective private networks and offer services to connected users. Consequently, the Internet is often the medium over which remote DoS attacks are initiated. Moreover, remote DoS attacks using the Internet may originate from all over the world and incorporate a large number of attacking Zombie drones. Local DoS attacks originate from within the network under attack. For example, an attacker may subvert a number of computers or sensor nodes on the local network and coordinate the subverted nodes to launch an attack on a local server providing critical network services such as security or local storage.

The research in this thesis focuses on DoS attacks targeted against WSN based HASs and the respective remote access approaches. Consequently, the remainder of this chapter provides a comprehensive analysis of the local and remote DoS threats and the current defences for WSNs and the respective remote access approaches.

3.3 Local DoS Attacks on WSNs

Recently, one of the most challenging research areas to receive attention in the field of network security is concerned with the investigation of local DoS attacks against WSNs and the design of WSN based DoS defence approaches and architectures. This section reviews the local DoS attacks identified in the existing literature and the potential defence approaches for protecting WSNs from local DoS attacks originating from within WSNs.

There are a number of approaches for classifying WSN based DoS attacks. (Raymond et al. 2008) and (Wood et al. 2002) propose the classification of DoS attacks based on the five-layer ISO model adopted by WSNs. The known DoS attacks are classified based on the protocol layer the attack targets. This includes the physical layer, data link layer, network layer, transport layer and the application layer. Consequently, this section adopts the five layer classification to review the varying WSN based DoS attacks and defences identified from the literature. A summary of the classification is provided in Table 3-1.

Table 3-1: WSN based DoS attacks and defences categorised by the targeted layer of the protocol stack, adapted from (Wood et al. 2004)

Layer	Attack	Defence
Physical Layer	Node Tampering or Destruction	Tamper resistant casing, camouflage
	Wireless Signal Jamming	Spread spectrum communications using frequency hopping, re-routing messages around affected areas
Link/Medium Access Control Layer	Collision	Spread spectrum communications using frequency hopping, re-routing messages around affected areas
	Interrogation	Link layer encryption, anti-replay mechanisms
	Packet Replay	Link layer encryption, anti-replay mechanisms

	Denial of Sleep	Link layer encryption, anti-replay mechanisms
Network Layer	Black Hole	Implicit acknowledgements, message duplication, use of multiple communication paths
	Hello Flooding	Geographic knowledge node authentication
	Cluster Head Attack	Encryption, anti-replay mechanism, authentication, and trust based cluster head election
	Homing	Message header encryption, dummy packets
Transport Layer	Flooding	Client puzzles
	De-synchronisation	Authentication
Application Layer	Environmental stimulus	Data Aggregation, and fixed sensing intervals
	Path-Based DoS	Unique secret keys for all nodes, secret key for each path, packet histories, rate limits, and one way hash chains
	Node Software Updates	Hash chain authentication, and cluster key authentication

3.3.1 Physical Layer DoS Attacks

There are two primary DoS attacks that target WSN nodes at the physical layer of the protocol stack. Firstly, due to the nature of many WSN applications nodes are often widely and openly distributed across large regions. Consequently, attackers are often provided with physical access to nodes, during which an attacker may tamper with a node with the intention of gaining access to confidential data contained on the node or subverting the node for performing other elicit activities on the WSN. Alternatively, an attacker may simply destroy nodes in an attempt to disrupt the functioning of the WSN or cause sensor blackouts where large portions of the WSN region remain unmonitored.

Although the destruction and tampering of nodes cannot be prevented, current defence measures focus on increasing the difficulty of node destruction and tampering, and decreasing the potential benefits of node destruction and tampering. In the case of node destruction, camouflaging nodes from attacker's sight and placing WSN nodes in tougher cases offers additional protection. Additionally, adding redundant nodes to the WSN infrastructure decreases the effect on network functionality from the destruction of a few nodes. In the case of node tampering, the existing defence measures include camouflaging nodes, and the placement of nodes in cases more resilient to tampering, and the use of self-terminating nodes, which wipe information from memory. The advantage of self-terminating nodes is to render tampered nodes useless to attackers.

Secondly, due to the wireless nature of WSN communications an attacker does not have to be in direct contact with a node to perform an attack. Instead, an attacker may launch an attack from a safe distant unobserved and potentially unnoticed by those under attack. The primary physical layer attack against WSNs is the jamming attack (Raymond et al. 2008). (Xu et al. 2005) categorises jamming attacks as constant, deceptive, random, or reactive.

In a constant jamming attack, the attacker continuously floods the victim's frequency range, leading to the corruption of packets transmitted between legitimate nodes on the victim's WSN. In a constant jamming attack, the attacker requires significantly more power than the victim network over a long period, or the attacker risks exhausting its power supply and so ending the attack. Consequently, a long-term constant jamming attack is not normally effective if the attacker is under the same constraints as the victim's WSN.

In a deceptive jamming attack, the attacker sends a constant stream of bytes into the network instead of a random signal. Causing nodes in many WSNs, such as TinyOS based WSNs, to remain in receive mode and never enter transmission mode.

In a random jamming attack, the attacker employs constant or deceptive jamming. The attack differs in that the attacker performs the jamming attack at random intervals for random durations and sleeps for the remainder of the time.

This conserves a significant amount of the attacker's power compared to constant and deceptive jamming alone, increasing the duration over which an attack may occur. However, during periods where the attacker is sleeping the communication abilities of the victim's WSN return to normal.

In a reactive jamming attack, the attacker monitors the radio frequency of the victim's WSN for traffic. Once traffic is detected, the attacker starts a constant or deceptive jamming attack. The reactive jamming approach saves the attacker a considerable amount of energy compared to constant or deceptive jamming alone. Moreover, the level of difficulty for detecting the attack is increased because the packet losses may mimic normal packet loss due to normal network packet collisions. Furthermore, the reactive attack provides more consistent blocking of normal network communications, although random jamming may provide a greater energy saving for attacks against WSNs with a higher level of network traffic, which keeps an active attacker constantly engaged.

The primary defence against jamming attacks is spread spectrum communications. The technique uses frequency hopping to spread communications across a larger frequency range than that taken by the original data to overcome jamming attacks that target a single frequency. For an attack to be effective against a node employing spread spectrum communications, the attacker must continuously switch the frequency jammed to match that of the victim or flood the whole frequency range. The additional scanning and channel hopping or brute force flooding of the whole frequency spectrum, if possible, significantly increases the rate of energy consumption for the attacker. Consequently, spread spectrum technology has been widely adopted and proven as an effective defence against jamming attacks. For example, spread spectrum communications have been adopted in wireless standards such as Bluetooth (Salonidis et al. 2005) and shown through extensive, practical real world use to offer sufficient protection. However, low cost, resource limited WSN nodes primarily consist of simple radios incapable of using spread spectrum communication techniques. Consequently, alternative defence approaches appropriate for resource limited WSNs have been suggested including placing victim nodes to sleep, and routing traffic around regions experiencing a jamming attack. In the first instance, placing nodes under a jamming attack to sleep,

waking only to detect if the jamming attack has stopped, allows the victim node to protect energy resources and resume normal operations once the jamming attack has ended. However, during the attack the whole region under attack is placed in sleep state, blocking network functionality and achieving the attacker's objectives of denying services to legitimate users. Alternatively, defences focused on maintaining network functionality during jamming attacks have emerged. These defences operate at the network layer, building on existing routing algorithms and routing communications around areas suffering from jamming attacks. For example, TinyOS Destination-Sequenced Distance Vector Routing continuously measures the quality of communication routes and directs traffic to avoid low quality communication paths, avoiding areas suffering from jamming attacks.

3.3.2 Link/Medium Access Control Layer DoS Attacks

The link layer hosts the MAC protocols employed by nodes to gain access to the communication medium and communicate with neighbouring nodes. Attackers exploit the link layer and associated MAC protocol to prevent legitimate nodes from gaining access to the network's communication medium. There are four primary DoS attacks against WSNs at the link layer including collision, interrogation, packet replay and denial of sleep attacks (Raymond et al. 2008).

The collision attack attempts to prevent legitimate messages from reaching the intended destination by sending packets from an attacker during the communication period of a legitimate user, thus causing packet collisions. If a collision attack is significantly strong, most packets sent from a legitimate user will collide with attack packets and fail to reach the intended destination. Moreover, the effect of packet collisions for MAC protocols employing backoff periods is considerably worse. An attacker may increase the backoff period of the victim, decreasing the victim's availability, with little expense to itself. The collision attack is similar to the PHY layer based reactive jamming attack. Consequently, the defences against this attack are also the same.

The interrogation attack exploits the request-to-send/clear-to-send (RTS/CTS) handshake employed by many MAC protocols to overcome the "hidden node problem" (Rahman et al. 2006) and establish a communication connection. An

attacker may continuously send RTS messages to elicit CTS replies from the victim, diminishing network bandwidth and the victim's resources. Alternatively, an attacker may continuously broadcast CTS messages, with long duration fields, in an attempt to fool neighbouring nodes that the communication medium is congested. The standard defence against the interrogation attack is strong link layer encryption to detect bogus RTS or CTS messages and the use of a cryptographically secure pseudo random number generator to provide secure nonce values for use with an anti-replay mechanism. The anti-replay mechanism prevents the attackers from replaying captured valid RTS or CTS values to overcome message encryption. Moreover, the use of the anti-replay mechanism overcomes the general threat of replayed messages sent to diminish the victim's resources. However, victim nodes still consume resources in receiving the RTS, CTS or general messages, due to the added requirement to decrypt all incoming messages. Nevertheless, the effectiveness of the interrogation attack is significantly decreased.

The denial-of-sleep attack was first identified by (Stajano et al. 1999), although at the time the attack was termed "sleep deprivation torture" attack. Since the denial-of-sleep attack was first discovered, a number of studies have been conducted into the effects of the attack on WSNs. The studies state that a denial-of-sleep attack is an attempt to quickly exhaust a nodes energy supply by keeping the nodes transceiver active and preventing it from entering sleep mode (Raymond et al. 2008).

Most denial-of-sleep attacks, targeted at the link layer of the protocol stack, focus on exploiting the MAC protocols that operate at the link layer. The MAC protocols control the period a transceiver remains active and inactive (sleep mode). Furthermore, most WSNs incorporate MAC protocols that are energy aware and designed to keep the WSN nodes in sleep state for as long as possible, whilst not affecting the nodes functionality, to extend the lifetime of the WSN. Accordingly, the MAC protocols make an attractive target for an attacker, because the transceiver consumes more energy than any other component on most WSN nodes. Consequently, subversion of the node's transceiver control mechanism allows the nodes energy supply to be quickly exhausted.

As a result, the denial-of-sleep attack is one of the most effective methods for conducting a DoS attack against a WSN. Other DoS attacks such as jamming attacks may take months to completely exhaust the energy supply of a node, whereas a denial-of-sleep attack may exhaust the energy supply of a node within a few days (Raymond et al. 2008). Moreover, the attack costs relatively little in terms of consumption of the attackers resources compared to those of the victim.

(Raymond et al. 2008), (Law et al. 2005), and (Raymond et al. 2009) evaluate the vulnerability of Sensor MAC (S-MAC), Berkley MAC (B-MAC), Timeout Mac (T-MAC), and Gateway MAC (G-MAC) to denial-of-sleep attacks. These energy efficient MAC protocols provide a representative sample of current WSN MAC protocols (Law et al. 2005), allowing for the assumption that weaknesses in these protocols may be present in other MAC protocols not evaluated. The following section provides a summary of the analysis of the most popular MAC algorithms to denial of sleep attacks.

The S-MAC protocol mediates access to the WSN's communication medium by dividing time into slots of 1300ms. Each time slot is divided into a sleep period and a wake period. The default setting of the S-MAC protocol puts each sensor node to sleep for 90% of the slot period, only waking for 10% of each slot period to communicate, significantly improving the lifetime of the WSN. In S-MAC a new node listens for a period of time to receive a SYN packet, to help the new node synchronise sleep and wake slots with neighbouring nodes. If no SYN packet is received after a period of time the new node emits a SYN packet allowing neighbouring nodes to synchronise with the new node. If a node receives two different SYN packets, the node synchronises with both nodes. An attacker may attempt to spoof SYN messages encoded with a sleep delay longer than that of the whole time slot. Resulting in neighbouring nodes failing to enter sleep mode, quickly exhausting the nodes power supply. However, the use of strong link layer encryption and anti-replay mechanisms, as previously discussed, provide an effective defence against this attack. However, encryption and anti-replay mechanism do not provide protection against subverted nodes in possession of cryptographic material, using spoofed SYN packets encoded with the correct cryptographic material.

The T-MAC protocol follows the same methodology as the S-MAC protocol for the synchronisation of nodes. However, incorporates an "adaptive time out" mechanism whereby nodes incorporate a time-to-sleep counter, if a node finishes counting down the time-to-sleep counter and has not detected any network traffic the node goes to sleep. T-MAC requires nodes to transmit during the start of the active portion of the time slot. If the node detects network traffic before the node has completed counting down the sleep counter, the node receives the message and resets the sleep counter, the process is repeated until no network traffic is detected and the sleep counter finishes and places the node into sleep mode. Consequently, an attacker may transmit or replay a constant stream of small packets to keep the nodes permanently active. As with the S-MAC protocol, link level encryption and anti-replay mechanisms can be adopted to protect against this type of attack.

The B-MAC protocol does not require synchronisation of neighbouring nodes to establish a communication link, unlike other MAC protocols such as S-MAC. Instead nodes in a network employing the B-MAC protocol use a method called "low-power listening" wherein nodes periodically check the wireless channel to see if any node wishes to communicate. Transmitting nodes broadcast a preamble longer than the check interval employed by neighbouring nodes to check if any node wishes to communicate. This allows all of the neighbouring nodes to detect the transmitted preamble. During a node's wakeup and check phase, if no transmitting node is detected the node goes back to sleep mode. However, if a preamble is detected indicating a node wishes to communicate the receiving node establishes a connection with the transmitting node, potentially using the earlier discussed RTS/CTS methodology, and waits to receive the message. Once the message is received the receiver repeats the sleep and check cycle. (Polastre et al. 2004) showed that under ideal conditions, B-MAC could have duty cycles as low as 1% in a low-traffic network providing for a very energy efficient MAC protocol. An attacker may transmit an unauthenticated stream or a stream of replayed broadcast packets to act as a preamble, causing legitimate WSN nodes to stay awake. (Raymond et al. 2008) state that an attacker instigating such an attack can keep B-MAC nodes awake for, on average, half the network lifetime. Again, link layer encryption, and anti-replay mechanisms help to overcome such attacks.

The G-MAC protocol adopts a frame-based approach for the coordination of communication within a WSN cluster. G-MAC divides time into different frames and each frame into a collection period and a contention free period. During the collection period or "contention period" nodes which have data to transmit to within the cluster send a future request to send (FRTS) message to a gateway node (cluster head). Moreover, nodes that have data to transmit destined for nodes outside the cluster, send the data to the gateway node using a standard RTS/CTS/DATA/ACK approach (Raymond et al. 2009). During the contention free period the gateway node broadcasts a gateway traffic indication message (GTIM), used for synchronisation of cluster nodes and to provide a schedule of message transmissions between members of the cluster. The gateway or cluster head in a G-MAC network is chosen through a periodic election process, resulting in the node with the most resources acting as the gateway. If the standard G-MAC approach is used without link layer encryption and anti-replay mechanisms, the protocol is vulnerable to attacks. An attacker may imitate the gateway and using faked GTIM messages force all nodes in a cluster to stay active all of the time, resulting in a reduction of the network lifetime. Experiments conducted by (Raymond et al. 2009) into the effects of DoS attacks against WSNs not employing link layer encryption and anti-replay mechanisms showed that a denial of sleep attack could lead to a reduction in network lifetime of up to 97% (12 days for WSNs under a DoS attack compared to a normal network lifetime of 371 days). However, even with the use of encryption and anti-replay mechanisms the FRTS packet must be received by the gateway and checked to see if it is authentic. Consequently, the gateway will disregard FRTS packets that fail to authenticate, however the authentication process will slowly deplete the gateways energy levels, although at a greatly reduced rate.

Denial-of-sleep attacks focus on keeping the transceiver active, which exhausts considerably more power than attacks targeting other aspects of the node such as processing or sensing. Thus, the advantage of denial of sleep attacks includes the ability to launch longer, more intelligent, reactive attacks against WSNs, avoiding the need for traditional energy expensive jamming attacks. All of the reviewed MAC protocols highlight the vulnerability of MAC protocols, in their native form, to denial of sleep attacks. Moreover, even with the adoption of encryption and anti-replay mechanisms the analysis of MAC protocols adopted by a

WSN can provide an attacker with valid information on how and when to launch attacks. Furthermore, cryptographic defences are only useful against outsider nodes or insider nodes designed to wipe cryptographic material during node tampering attacks. If an attack is launched, from a subverted node with access to cryptographic material, such as encryption keys and nonce values, cryptographic defences are rendered practically useless. Additionally, the literature review has revealed little research on the effectiveness of denial-of-sleep, and more generally DoS, attacks from subverted insider nodes targeting MAC layer protocols and little evidence of defences against such attacks.

3.3.3 Network Layer DoS Attacks

DoS attacks targeted at the NWK layer of the communication protocol stack seek to disrupt the routing of messages between members of the WSN (Raymond et al. 2008). General network level attacks include the spoofing, replaying or altering of messages as they are routed through the WSN. The most common forms of these attacks include black hole attacks, hello flooding attacks, cluster head attacks, and homing attacks. Following is a summary of these network layer attacks, together with the normal defence measures used against these attacks where available.

In a “Black hole attack”, a subverted routing node makes itself part of many communication paths and then drops either all packets it receives or selectively drops packets to avoid detection mechanisms. Defences for black hole attacks include:

Implicit acknowledgements, which make sure messages are forwarded as intended. However, this approach requires the transceiver of the source sensor node to remain active to verify acknowledgements from router nodes along the message path. This places an additional burden on the energy resources of the already resource limited sensor node sending the message. Alternatively, the same message can be duplicated and sent through multiple routes across the WSN to the destination node, increasing the chance that at least one of the paths will avoid the subverted routing nodes. However, this approach wastes the WSNs already limited energy, processing, and bandwidth resources. Firstly, a number of redundant communication paths have to be engineered into the network. Secondly, the total

amount of energy required to send a message across the WSN is increased a number of times. Due to the resource-limited nature of WSNs, incorporating redundant paths into a WSN may not be feasible. Furthermore, energy conservation is one of the most important considerations in the design of resource limited WSNs. Consequently, neither of these defence approaches offers an attractive solution, for resource limited WSNs.

During a "Hello flooding attack", an attacker exploits routing protocols that advertise the existence of a node to one-hop neighbours through the broadcast of hello messages. In the case of a "Hello flooding attack" the attacker is a relatively resource rich node (e.g. a laptop) with a greater transmission range than nodes from the WSN under attack. During the initial stage, the attacker intercepts a valid hello message broadcast from a legitimate node. During the next stage of the attack, the resource rich attacker replays the earlier intercepted hello message to nodes outside the one-hop transmission range of the node from whom the hello message was originally intercepted. Consequently, nodes from outside the one-hop communication range of the source of the original hello message form nonexistent communication links with the original node. When these nodes attempt to route message to the original node they are unsuccessful. To defend against hello flooding attacks, legitimate nodes must either have prior knowledge of the WSN topology or verify nodes are within one-hop before adding them to routing paths. Location-based routing protocols have prior knowledge of the structure of WSNs (Santos et al. 2006) and can ignore hello messages from nodes known to be outside a one-hop communication range. Alternatively, nodes can authenticate the source of a hello message in a three-way handshaking process before adding a node to its routing path.

For ease of management, improved energy efficiency, and reduced bandwidth requirements large scale WSN's often adopt clustering topologies. In a cluster topology, a WSN is logically split into clusters (groups) of nodes. Each cluster has one node, which plays the role of a cluster head. The cluster head is the point of ingress between different clusters and the point at which all data from a cluster is aggregated before being routed towards the destination cluster. This reduces the amount of duplicated messages sent across the network as well as

incurring less transmission energy cost per sending node. The process of choosing a cluster head varies based on different routing protocols. However, in general a number of nodes volunteer to act as a cluster head. The nodes advertise their resources including how much energy they have and their current transmission power. The nodes with the higher level of resources are chosen as the cluster heads.

An attacker may launch a "Cluster Head Attack", where a subverted node either advertises more resources than it poses, such as a higher power level, in order to get as many nodes in the WSN to pick it as their cluster head. Alternatively, a relatively resource rich attacker, such as a laptop, may use its higher transmission power to be selected as the cluster head, or a node may capture and replay messages from other nodes volunteering to be the cluster head. Once a subverted node is chosen as the cluster head, it may choose not to route any received messages or it may randomly drop messages in order to evade detection by DoS defence mechanisms.

As with the other DoS attacks discussed in this section, the encryption of messages, the use of an anti-replay mechanism, and the authentication of messages including volunteer messages from potential cluster head nodes helps to protect against cluster head attacks. However, cryptographic mechanisms alone are not sufficient to provide protection against subverted nodes with access to valid cryptographic material. To overcome the threat of a cluster head attack, schemes for electing a cluster head have been proposed, instead of the current approach of allowing nodes to volunteer as the cluster head. However, many of the election-based schemes rely on the cluster nodes providing correct information about their resources (Crosby et al. 2006). A subverted node may manufacture a message with falsified data concerning its resources, encrypt the message with valid cryptographic material, broadcast the message to neighbouring nodes and be selected as the cluster head based on the falsified data. For example, (Crosby et al. 2006) proposed a secure process for electing cluster heads based on an asymmetric trust based approach, where nodes use cluster-wide and pair-wise public key cryptography to authenticate potential cluster head nodes. However, this scheme does not protect against subverted nodes with access to cryptographic material such as the public keys. Furthermore, the use of asymmetric cryptography adds a significant burden to

resource limited WSNs. Moreover, the use of a large number of pair-wise and cluster-wise keys may not be feasible for large scale WSNs.

Other, more sophisticated attacks target key nodes in a WSN such as the WSN coordinator, gateway node, cluster heads, and trusted third party nodes to cause widespread disruption across the network. The difficulty in performing such attacks arises from the identification of the key nodes in a WSN. "Homing attacks" analyse network traffic to identify traffic patterns that may point to key nodes. Once key nodes have been identified, the attacker launches a DoS attack, such as those previously discussed, on the key nodes causing the maximum disruption to the WSN for the least effort. There are two primary approaches for tackling traffic analysis in WSNs. Firstly, the encryption of message headers can prevent eavesdroppers from identifying the destination of an intercepted message. However, on a relatively small scale WSN an attacker can observe different volumes of traffic across the whole network to identify key WSN nodes. The use of dummy packets to normalise the network traffic volume across the WSN has been proposed (Deng et al. 2004). However, this wastes a significant amount of bandwidth and energy. Consequently, it has been suggested this approach should only be used when the prevention of traffic analysis is crucial (Raymond et al. 2008).

This section has reviewed a selection of the most popular NWK layer WSN attacks and the current defence mechanisms against these attacks. Link layer authentication and anti-replay mechanisms have been shown to be an effective defence against most NWK layer attacks. However, there are certain NWK layer attacks, such as Homing attacks, which do not require cryptographic measures to be overcome, which remain significant challenges. Moreover, the defence measures reviewed do not provide protection from DoS attacks originating from subverted nodes with access to cryptographic material.

3.3.4 Transport Layer DoS Attacks

The focus of transport layer DoS attacks is to exploit communication protocols that use connection oriented communications and maintain connection information. The main transport layer attacks against WSNs include "De-synchronisation attacks" and "Flooding attacks".

During a "De-synchronisation attack", an attacker targets active communications employing connection oriented communication protocols and modifies or forges the parameters of captured messages, such as control flags and sequence numbers. The modified or forged messages are introduced back into an active communication stream between two participants (Yang et al. 2008). Consequently, when modified or forged messages arrive at their respective destinations they are rejected as out of sequence or as corrupted, leading to the sender retransmitting messages and wasting energy and network bandwidth. An intelligent attack may repeatedly forge or modify messages leading to legitimate messages being incorrectly rejected at the receiving node for the duration of the attack. The encryption of message headers or the whole message can prevent attackers from modifying existing messages and creating forged packets. Moreover, anti-replay mechanisms can prevent legitimate messages from being inserted into legitimate communication streams undetected.

Likewise, the targets of a "Flood attack" are networks employing connection oriented communication protocols. The attacker requests a connection from a node in the WSN, the node reserves space in its open connection buffer and sends a SYN acknowledgement. At this point, the attacker should respond with an acknowledgment completing the connection in a three-way handshake. However, the attacker does not respond leaving the victim node waiting for an acknowledgment. After a period of time has passed a timeout counter expires causing the victim to clear its open connection buffer. However, an attacker may repeatedly request a number of connections and leave them half open, exhausting the victim's connection buffer, and preventing legitimate connection requests for the duration of the attack (Yang et al. 2008). One approach for protecting against flooding attacks in WSNs requires connecting nodes to complete a complex puzzle before a node reserves connection space (Wood et al. 2002). This approach assumes that an attacker has limited processing resources to solve complex puzzles. Consequently, at any given moment in time the number of half-open connections any attacker can establish is considerably reduced. Furthermore, in the case of resource limited WSNs, where an attacker may have the same resources as the victim, the complex puzzle defence may render flooding attacks unfeasible. However, the use of complex puzzles requires all nodes in the WSN to have

additional hardware to solve complex puzzles. Moreover, each connection attempt will incur legitimate hosts additional energy and processing costs. Making complex puzzles a prohibitively expensive defence approach for resource limited WSNs, where conserving energy is often a primary concern.

3.3.5 Application Layer DoS Attacks

Attacks targeted at the application layer of WSNs either focus on weaknesses in application software specific to a particular WSN or focus on more general inherent weaknesses in the application layer of WSNs. Attacks targeting inherent weaknesses are far more common because the potential number of victims is far higher for the effort of developing an attack strategy. The most popular forms of application layer attacks include “Environmental Stimulus attacks”, “Path-Based DoS attacks” and “Node Re-Programming attacks”.

Environmental stimulus attacks aim to exhaust the power resources of victim nodes and overwhelm other network resources. The attack requires the attacker to know the environmental characteristic the victim’s WSN is sensing (i.e. carbon monoxide levels) and generate stimuli (i.e. carbon monoxide), causing sensing nodes to transmit large volumes of sensed data towards a base-station. This results in the increased consumption of energy directly at the sensor node and across the communication path between the victim node and base-station. Moreover, if a sufficient number of nodes are targeted the high volume of sensed data forwarded towards the WSN base-station may overwhelm the communication paths and the base-station, resulting in a network wide failure of services. However, this form of attack is only valid for WSNs designed to transmit data as soon as the data is sensed. WSNs designed to transmit data at regular intervals, regardless of stimuli are immune to such attacks. Moreover, WSNs that aggregate and remove duplicated data before transmission significantly reduce the effectiveness of such attacks.

During a path-based DoS attack an attacker floods fake or replayed packets along a multi-hop, end-to-end routing path. The attack quickly consumes the resources of nodes along the communication path and prevents nodes downstream from the path under attack from communicating with the base-station. Thus, a path-based DoS attack can affect a much greater portion of a WSN, than just the path

under attack (Deng et al. 2005). There are a number of methods proposed for defending against path-based DoS attacks, the primary role of most defence approaches is to detect and remove spurious packets along a communication path. (Deng et al. 2005) proposes four generic defence approaches against such attacks:

1) Each node along a communication path shares a secret key with the sender. The sender generates authentication and integrity material for each key/node and appends it to each packet. Consequently, each packet is validated at each hop along the communication path, all the way to the destination. This approach requires each node in the network to pre-share a secret key with every other node along every potential communication path in the whole WSN. The resource-limited nature of WSNs makes the storage requirements of this approach infeasible for most WSNs. Moreover, the small size of packets in WSNs makes the addition of so much authentication information with each packet impractical.

2) A modified approach, to that discussed in (1), involves a node storing a path key for every potential path in a WSN. Although, the storage cost of this approach is much lower than the previously discussed approach, the storage requirement on each node for large networks is still significant. Moreover, if any one of the nodes in the network is subverted an attacker can flood a whole communication path. As previously discussed, this may affect a much larger region of the WSN than the communication path under attack alone. Additionally, in ad hoc WSNs where nodes may leave and join the network throughout the lifetime of the WSN, the process of updating the path keys of nodes is not a straightforward process.

3) An alternative approach to identifying replayed packets though non-cryptographic means, involves each node maintaining a history of all prior packets and comparing all incoming packets with the historical list of packets. This approach although effective is not feasible for resource limited WSN nodes with limited storage resources.

4) Rate control mechanisms can also be applied to each node, limiting the amount of replayed packets accepted from any one node. However, due to the nature of WSN, certain nodes such as nodes directly around a coordinator or router nodes have different packet rates. Moreover, depending on the application of the WSNs, the packet rate may change for different time periods. Additionally, the addition of new nodes and the removal of old nodes requires packet rate statistics to be periodically re-calculated. Thus, rate limits although effective are not necessarily feasible for WSNs (Deng et al. 2005).

In addition to these four categories a number of approaches including (Deng et al. 2005) and (Li et al. 2007) have adopted one-way hash chains to protect against path-based DoS attacks. In the hash-chain based approaches, a node hashes a random number repeatedly storing the value of each hash in a chain so producing a hash chain. The last hash value (n) produced is distributed to all nodes in the nodes communication path. Each node has access to the hash algorithm employed. However, it is not feasible for an attacker to derive the value which when hashed forms the shared hash value (n). The next message contains the previous hash value in the chain (n-1), from which (n) was derived, only the node which has access to the original hash chain can include this value. The recipients apply the pre-shared hash function to the hash received (n-1), if the previous hash (n) can be derived the message is considered valid and not a replay. Moreover, if an attacker intercepts the hash value (n-1) it is different to the next hash value that will be sent from the hash chain (n-2). Consequently, hash chains offer a lightweight approach for protecting against path based DoS attacks, which involve the replay of legitimate packets. The problem with certain hash-chain approaches such as those adopted by (Perrig et al. 2002) and (Liu et al. 2003) is that they require the time synchronisation of nodes in the WSN. However, this is not practical for large scale WSNs, where complicated maintenance schemes are required to keep all nodes synchronised. For example, complex maintenance schemes are required to deal with situations, such as dropped packets where some of the nodes in a path receive a new hash value and some do not. In this situation, if a sender replays a dropped message the intermediate nodes, which have already received the hash value, will reject the message as a path-based DoS attack. If the sender appends the next value in the hash chain to a message, the

nodes in the path that did not receive the last hash value, will reject the message as a path-based DoS attack. However, simulations of such schemes (Deng et al. 2005) show promise in the feasibility of such approaches for use with WSNs, however considerably more research is needed in this area to experimentally test the feasibility of such schemes with practical applications of WSNs.

Once a WSN is deployed, it may be necessary to update the software contained on some or all of the associated WSN nodes, due to bugs or technological advances. Due to the nature of many WSN applications where nodes are located in inaccessible and remote locations it is desirable to remotely and wirelessly update node software. The process of updating node software is referred to as code dissemination. There are numerous approaches and protocols for disseminating software, such as the approach adopted by TinyOS called Deluge. In the Deluge approach, nodes periodically send advertisements containing their software version. Nodes check the advertisements received from neighbouring nodes. If a neighbouring node has a later software version a request is sent to the node for the latest software update. In the Deluge approach, an image of a software update is split into equally sized pages, and each page is split into equally sized packets. The pages are then delivered to the destination nodes in sequential order. Once a node receives a complete new page, the node acknowledges the receipt of the page and requests the next page. The Deluge and other software dissemination approaches normally assume a trusted environment and offer little or no security services. Consequently, there is little protection from attackers wishing to subvert the software update process. As a result, secure methods for reprogramming nodes have emerged, one such scheme is called Seluge (Hyun et al. 2008), a secure extension of the Deluge approach. The Seluge approach addresses several weaknesses in the Deluge approach. Firstly, in the deluge approach a whole page has to be received before it is validated, consuming significant energy resources and offering a potential target for attackers. The Seluge approach adopts a hashing mechanism, which imprints each packet in a page with a hash code. The hash code is checked on arrival at a node allowing forged or corrupted packets to be detected at an early stage. Similarly, Seluge adopts cluster key based authentication for software version advertisements and software update request messages to overcome DoS attacks based on spoofed messages. Moreover, one-way-hash chains are adopted to

authenticate pages instead of signatures, overcoming attacks aimed at exhausting the energy resources of nodes through the generation of multiple, energy expensive, signature authentication requests.

This section has presented an extensive review of DoS attacks originating locally from within WSNs. These attacks can cause a serious disruption to WSN communications and to remote users attempting to access WSN services. The next section reviews the remote DoS attacks that originate from outside of the WSN, and attempt to disrupt communications on the WSN for local and remote users, and DoS attacks that target the remote access infrastructure of WSNs to disrupt communications for remote users. It should be noted that due to a lack of research focused on remote DoS attacks that focus exclusively on WSNs, the following section examines the most popular remote DoS attacks that have been perpetrated against LAN, however can easily be implemented against any other network, such as WSNs.

3.4 Remote DoS Attacks on WSNs

It has been suggested that regardless of how well local security mechanisms protect potential victims, ultimately the victims susceptibility to DoS attacks depends on the effectiveness of security mechanisms across the connected networks, including public networks such as the Internet (Mirkovic et al. 2004). Consequently, protecting relatively resource poor WSNs from attackers who wield the power of large, relatively resource rich, yet DoS vulnerable public access networks poses significant research challenges. Attacks, such as these, which originate from outside the victim's network are termed remote DoS attacks (Kumar et al. 2006). This section and research outlined in the Thesis focuses on remote DoS attacks originating from the Internet. This is due to the worldwide dominance of the Internet as the public access network of choice for communicating over large distances.

There are three main objectives of a remote DoS attack. Firstly, a DoS attack may disrupt communications across a WSN and prevent local nodes from communicating and accessing local services such as trusted third parties. Secondly, an attack may attempt to overwhelm the point of ingress between the Internet and

WSN, in an attempt to block legitimate users from remotely accessing the WSN. Thirdly, an attacker may attempt to disrupt the WSN's remote access infrastructure to prevent remote users from accessing the WSN. In the case of many WSN applications, the sole objective of a WSN is to monitor a remote environment and report sensed data to a remote destination. Consequently, remote DoS attacks that block legitimate users from accessing a WSN, in a timely manner, effectively render the WSN ineffective and as such pose a significant research challenge.

3.4.1 Remote DoS Attacks

There are numerous approaches for conducting a remote DoS attack over the internet and against local networks such as WSNs. A summary of some of the most popular remote DoS attacks follows. The attacks are categorised based on those, which exploit vulnerabilities in networks such as application software bugs and flaws in underlying protocols and those, which adopt a brute force approach in an attempt to overwhelm a victim's resources.

3.4.1.1 Vulnerability Based DoS Attacks

As previously discussed, vulnerability based attacks exploit known flaws in networks, including flaws in systems hardware, flaws in protocols, and bugs in application software. The most widely known and popular vulnerability based DoS attacks include TCP SYN, NAPTHA and Teardrop attacks.

The TCP SYN attack was first identified by Bill Cheswick and Steve Bellovin in 1994 (Mahimkar et al. 2007). In a TCP SYN attack, during the three-way TCP handshake between a client and server, the client requests a connection from a server. The server responds by allocating sufficient buffer space, in the server's half-open connection buffer and transmits an acknowledgement and nonce (random number) to the client. At this stage of the three way handshake the client should increment the received nonce and respond with an acknowledgment and the incremented nonce, at which stage the server moves the connection from the relatively resource limited half open connection buffer to the, relatively resource rich, open connection buffer. In the TCP SYN attack, when the client receives the acknowledgment and nonce from the server, the client fails to complete the connection with the server. The server continues to reserve the allocated buffer

space for a certain period of time. The attacker repeats the aforementioned steps numerous times from varying sources until the servers half open connection buffer resources are overwhelmed (Wang et al. 2002).

The TCP SYN attack aims to prevent the server under attack from providing services to legitimate clients by exhausting the servers half-open connection buffer resources. In the case that the server under attack is a gateway server between a WSN and the Internet, the attack aims to prevent the server from providing legitimate users with access to the respective WSN.

To prevent a single host from performing a TCP SYN attack and creating multiple half-open connections, the number of TCP connections a single host can establish in a given period is limited by many servers. Consequently, for an attacker to launch a successful attack and open multiple half-open connections, the attacker must either spoof the IP address of different TCP SYN requests to appear as though the requests are coming from different sources or the attacker must use a large number of hosts to perform the attack. The TCP SYN attack is almost identical to the earlier described "flood attack", which is launched locally from within WSNs (See Section 3.3.4). Consequently, the defences against TCP SYN attacks using spoofed IP addresses or originating from a large number of hosts are similar to those employed against flood attacks. The six most common TCP SYN attack defences adopted by many systems are as follows.

Firstly, "ingress filtering" is used to identify and reject TCP SYN requests originating from spoofed IP addresses. There are different methods for performing ingress filtering; a review of them all is outside the scope of this thesis, for more information please refer to (Baker et al. 2004). However, the underlying principle of ingress filtering is to check the source address of incoming packets against a predefined list of acceptable addresses. For example, an ISP (Internet Service Provider) is aware of the IP addresses used as part of its network. Consequently, packets leaving the ISPs network with spoofed addresses that could not have originated from within its network can be easily spotted and removed. However, packets from subverted hosts within a network or from spoofed packets with addresses within the range of the local network are not detected using ingress

filtering. Consequently, the closer the ingress filter is to the source of the attack the more accurately spoofed addresses can be detected.

Secondly, the half-open connection buffer resources of victims can be increased to handle larger TCP-SYN attacks. However, this approach is limited because the size of any potential TCP SYN attack is unknown. Consequently, the potential for a large enough TCP SYN attack to overwhelm a victim's resources remains.

Thirdly, the duration before a half open connection is timed out at the victim's server can be decreased. This leads to half-open connections being terminated faster and resources at the half-open connection buffer being released faster. Although, this method increases the difficulty of launching a TCP SYN attack, the potential for an attacker to increase the rate of an attack to compensate for the reduced timeout period remains.

Fourthly, instead of a server reserving buffer space before the three-way handshake has completed, the server can wait until the handshake has been completed. One approach to achieve this is for the server to store a hash of secret bits received in a TCP request packet and the respective connection's IP address, in a SYN cache, instead of using a half-open connection buffer to maintain the connections state. In this approach, the server does not reserve any buffer space until the three-way handshake has been completed. Once the three-way handshake has been completed, the server uses the appropriate cached connection state to establish the connection. Although this approach is effective, a delay is added to the connection process. Moreover, an attacker may shift the focus of the attack from the server's half-open connection resources to the server's hash storage resources.

Fifthly, another approach involves the use of SYN cookies. The approach allows a server to retain no connection state information using its resources, instead the information is encoded and passed to the client as part of the nonce and stored on the client as a cookie. Once the three-way handshake has been completed, the connection is established using the information stored on the client side cookie.

Finally, one of the latest defences against TCP SYN attacks, involves the server requesting that the client completes a complex puzzle before a connection

space is reserved (Wood et al. 2002). This form of defence is very effective against attackers using spoofed IP addresses and presuming the attacker has limited computational resources, reduces the number of simultaneous connection requests possible from a single attacking client at any one moment in time. Moreover, the maximum size of an attack from a large distributed attack from a number of attacking hosts is considerably reduced. However, the use of client puzzles does slow down the connection setup process. Furthermore, the server issuing the puzzles also has to calculate the answer to the puzzles to verify the answers received from connecting hosts.

All of the defence mechanisms discussed increase the difficulty of carrying out TCP SYN based DoS attacks. However, most have drawbacks resulting in different mechanisms or hybrid combinations of these mechanisms providing the optimal solution for different applications.

During a NAPTHA attack, an attacking client opens a legitimate connection with a server and immediately closes the connection without sending the FIN/RST messages to the server. Resulting in the server maintaining the connection unaware the connection has been terminated by the malicious client. The attacker performs this attack from numerous Zombie machines, depleting the victim's resources and preventing legitimate clients from forming new connections. As with the TCP SYN attack, the objective of this attack is to prevent the victim's server from providing services to legitimate clients. Moreover, if the server is a gateway server between a WSN and the Internet the attack aims to prevent the server from providing legitimate users with access to the respective WSN. (Mahimkar et al. 2007) proposes an approach for tackling NAPTHA attacks called dFence. The approach involves a third party between the server and client responsible for monitoring the length of time a connection has been idle. If the time a connection has been idle exceeds a predefined threshold value, dFence terminates the connection with the server on behalf of the client. The disadvantage of the dFence approach is that legitimate connections might be incorrectly terminated.

The Teardrop attack (Microsystems 1998) was prevalent in 1997 and targeted computers running Windows 3.1, 95, and NT machines and Linux versions prior to 2.0.32. An attacker uses the Teardrop attack tool to send overlapping IP

fragments to the victim. A flaw in the software causes the victims TCP/IP fragmentation re-assembly code to incorrectly handle the overlapping IP fragments. The Teardrop attack causes vulnerable machines to crash or reboot, causing any active data in memory to be lost. Although the teardrop attack no longer poses a threat to most machines, it highlights how a simple flaw in an application can crash vulnerable machines, denying services to legitimate users. As with most vulnerability based DoS attacks the teardrop attack requires a significantly smaller sized attack to be effective than brute force attacks. However, a software update applied to vulnerable machines can prevent the teardrop and other vulnerability attacks.

3.4.1.2 Brute Force Based DoS Attacks

The underlying objective of all brute force attacks, also known as flooding attacks, is to overwhelm the victim's resources with higher levels of traffic than the victim's system is designed to handle. Thus, consuming the victim's resources, with malicious requests, and denying the service requests of legitimate users. There are numerous types of brute force based DoS attacks, however there are two broad categories of Brute Force attacks, direct attacks and reflector attacks (Chang 2002). This section reviews a selection of the most widely known direct brute force attacks such as UDP, and ICMP flooding attacks and reflector attacks such as the Smurf attack, and DNS reflector attack.

In a UDP flooding attack, a stream of UDP packets is transmitted to a victim host, exhausting the victims network bandwidth and consequently preventing UDP and other packets sent from legitimate users reaching the intended destination. Moreover, the UDP protocol is a connectionless protocol; as a result, in an intelligent attack where the IP address of each packet is spoofed, each packet must be accepted and checked before rejection. As a result, legitimate users are not able to effectively communicate with the victim during an effective DoS attack (Chang 2002). The potential defences for flooding attacks designed to exploit connectionless protocols, such as UDP, include statistical analysis approaches designed to detect and remove attack traffic. These defences are discussed in detail in section 3.4.2.

Similarly, in an ICMP flooding attack a stream of ICMP echo request packets are transmitted to a victim host, exhausting the victim's networks bandwidth. Moreover, the victim attempts to process the ICMP echo requests, consuming the victim's CPU time. Additionally, once the victim has processed an ICMP echo request the appropriate reply is sent, further exhausting the victim's already exhausted network bandwidth (Mirkovic 2003). Thus, legitimate users are prevented from effectively communicating with the victim. As with UDP attacks the defences for ICMP flooding attacks are discussed in detail in section 3.4.2.

Both UDP and ICMP flooding DoS attacks highlight two direct attacks. The attack traffic received at the victim end originates directly from the attacking zombie computers. In the case of reflector attacks, the attacking zombies send requests to legitimate servers that require responses from the server. The zombies spoof the IP address of the victim node in the request sent to the legitimate servers. Consequently, the servers reply to the requests, using the victim's IP address, and inadvertently flood the victim node with replies. Reflector attacks are harder to detect than direct attacks as the incoming flood of traffic is from a legitimate source (Paxson 2001). Moreover, the zombie machines from which an attack is launched are harder to trace because the legitimate servers used to reflect the attack might not record the details of the origin of requests they reply to. Two of the most widely known examples of flooding attacks that use reflectors are the Smurf and DNS reflector attacks.

During a Smurf attack, a stream of ICMP echo requests is sent to subnet broadcast addresses using the victim's spoofed IP address. Unlike the direct ICMP attack, the objective of a Smurf attack is not to exhaust the recipients of the ICMP echo requests. Instead, the objective of the attack is to send ICMP echo request to all nodes in a subnet, resulting in the respective subnet nodes generating responses to the ICMP echo requests targeted at the victim (Paxson 2001). The result of the attack is to overwhelm the resources of the victim, including flooding the victim's bandwidth, not only causing disruption to the victim nodes availability but also to all those nodes along the path of the DoS attack. The Smurf attack provides a good demonstration of reflector attacks. However, the Smurf attack has received much attention in research and there are simple steps that can be taken to prevent this

attack, such as ignoring requests to broadcast ICMP echo requests. As with direct ICMP attacks, other defences are discussed in detail in section 3.4.2.

During a DNS reflector attack, a stream of DNS look up requests is generated using the victim's IP address as the forged source of the request. The DNS lookup server performs the DNS lookup and returns the results of the lookup to the victim. The attacker repeats this process repeatedly for the duration of the attack, whilst simultaneously using multiple zombies to perform the same action. Consequently, the victim is overwhelmed with DNS lookup responses (Cheung 2006). As before the effect of the attack is to overwhelm the resources of the victim, including flooding the victims bandwidth, not only causing disruption to the victim nodes availability but also to all those nodes along the path of the DoS attack. The DNS reflector attack is particularly difficult to deal with at the DNS for two primary reasons. Firstly, unless the attack damages the DNS itself, there are few incentives to encourage the operators of the DNS to employ costly defences. Secondly, it is difficult to differentiate between legitimate and forged requests.

This section has reviewed some of the most popular and widely known remote DoS attacks. The approaches adopted to mitigate these attacks have been highlighted. The following section investigates the systems that have been proposed in academics and industry, adopting some of the previously discussed defence approaches, to combat the threat of remote DoS attacks.

3.4.2 Remote DoS Defences

The previous sections have outlined the most popular and widely known remote DoS attacks. There are numerous other known remote DoS attacks and in all likelihood, many more remote DoS attacks that will emerge as new vulnerabilities in old and new technologies are discovered (Mirkovic 2003). Due to the serious threats that arise from remote DoS attacks a significant amount of research has been conducted into developing methods for detecting and defending against remote DoS attacks. (Mirkovic 2003) introduces a taxonomy for classifying DoS attack defences based on the locality of the defence, the classification consists of DoS defences located at the victim, attacker source, and hybrid defences distributed at both the

victim end and attacker source. Following is a summary of the defences identified from the literature, categorised based on the previously discussed taxonomy.

3.4.2.1 Victim Based DoS Defence

The most widely employed DoS defences are located at the victim end of attacks (Xiang et al. 2006). Following is an updated selection of victim-based defences including resource multiplication, honeypots, NetBouncer, Synkill, and protocol scrubber as originally identified by (Mirkovic 2003).

During a brute force DoS attack the attacker attempts to exhaust the resources of the victim. To limit the damage of a DoS attack and reduce the impact of the attack on legitimate users the victim may increase the level of resources (such as adding more memory, increasing the systems processing power and increasing the systems bandwidth) to meet the demands of the DoS attacks and provide an acceptable level of service for legitimate users. This form of defence is called "Resource Multiplication". Moreover, the system may implement a fair usage policy to share the increased level of resources, amongst the systems users, further decreasing the impact of an attack on legitimate users. (Chiba et al. 2006) proposes such a defence system, which duplicates a server three times. Incoming packets are assigned the IP address of one of the servers based on the source domain of the packets. Once an association has been created, packets from a domain are routed to the same server for the duration of the communication. Packets from non-associated domains received at the servers are rejected. The proposed scheme and other resource multiplication schemes increase the difficulty of carrying out DoS attacks, such as UDP and ICMP flooding attacks. However, the potential for an attacker to increase the size of the attack and overwhelm the victims increased resources remains. Moreover, it may not be practical to duplicate the resources of low cost systems such as WSNs where low cost is a key design characteristic.

Remote DoS attacks rely on the attacker's ability to successfully send data and disrupt systems, such as web servers, providing services for legitimate clients. Honeypots have been proposed as a method for increasing the difficulty for an attacker to successfully send data to and disrupt a service providing system. A honeypot is a system that mimics the system it is protecting. The objective of a

honeypot is to lure attackers into believing they are connected with and attacking a real system and not the honeypot (Weiler 2002). The approach requires the honeypot to be able to distinguish legitimate network traffic from attack traffic and forward legitimate traffic to the real system, whilst responding to suspected attacks directly. There are numerous methods employed to authenticate users, (Das 2009) proposes a trust based scheme where authorised clients pre-share secret information for authentication purposes. To mimic response from the real system the honeypot may create a virtual model of the real network to respond to attackers or a parallel system may be created for responding to attacks. Additionally, to prevent a single honeypot from being overwhelmed and creating a point of failure further down the communication path certain approaches such as (Das 2009) incorporate multiple roaming honeypots. At any moment in time a number of the honeypots are legitimate forwarding clients, which forward data to the end destination. The remainder of the honeypots mimic the real network and respond to potential attack traffic on the real systems behalf. During the start of communications, the clients authenticate to a honeypot and receive a list of the honeypots that can be used for communications with the end destination. Consequently, data sent to the legitimate honeypots is forwarded to the real system. Whereas, data arriving at other honeypots is considered to be attack traffic and dealt with by the honeypots. Over a period of time the role of the honeypots is randomly changed to further increase the difficulty of the attacker guessing the correct honeypot required to access the real system. Honeypots add an additional layer of protection for vulnerable systems. However, the cost of adding honeypots may be prohibitive for low cost networks. Moreover, the potential for a powerful attacker to overwhelm the honeypots or the target systems Internet connection's bandwidth remains.

An alternative approach for tackling a brute force attack, where resource duplication is not possible is rate limiting. (Keromytis et al. 2002) defines rate limiting as a bandwidth restriction on a category of traffic such as ICMP, or UDP. During an attack, a rate-limiting algorithm drops packets either randomly or based on pre-defined rules. Rate limiting provides an effective defence against the exhaustion of a host's resources. However, due to the difficulties in identifying attack traffic from legitimate traffic, both suffer from rate limiting. A number of the

following defence approaches incorporate rate limiting in addition to novel DoS detection mechanisms.

As discussed earlier, packets originating from spoofed IP addresses increase the difficulty of tracing the source of DoS attacks and help attackers evade IP based DoS defences, such as the resource multiplication approach proposed by (Chiba et al. 2006). As previously discussed, ingress filtering is the conventional defence against IP spoofing. Whereby, the source of packets is verified to filter out nonexistent, spoofed IP addresses close to the source of the attack. An alternative approach involves sending a message to the source of the packet and waiting for a response, to verify that the source exists and that the packet was sent from there. (Thomas et al. 2003) proposes NetBouncer, an approach for ascertaining the validity of the IP address of incoming packets. NetBouncer intercepts incoming packets and sends an ICMP ECHO request, containing a hash value, to the IP address of the incoming connections. If an ICMP ECHO message is returned from the client containing the correct hash value the client is considered valid and added to a list of valid clients. Future connections from IP addresses contained on the legitimate list of clients are not validated. The hash value allows attackers spoofing the IP address of legitimate machines to be detected. The innocent ECHO responses from legitimate hosts will not contain the correct hash code. Additionally, NetBouncer incorporates the client puzzle based TCP SYN attack defences, discussed earlier. The NetBouncer system primarily provides a low cost and scalable solution for providing defences against DoS attacks incorporating spoofed IP addresses. However, the system does not provide protection against attacks using zombies using legitimate IP addresses.

As previously discussed, weaknesses in the TCP protocol have given rise to DoS attacks designed to exploit TCP weaknesses. One resource duplication based approach to defend against the TCP SYN attack is Synkill. The Synkill (Schuba et al. 1997) approach performs active monitoring of all packets on a network and has the ability to inject new packets into a network. Synkill acts as a gateway between a client and server. The attacking client requests a connection with a server. Synkill intercepts this request and forms a connection with the server on behalf of the client. Synkill then responds to the clients TCP connection request and waits for the client

to complete the three-way handshake. Consequently, moving the connection from the resource limited half-open connection buffer to the larger resources available for established connections. After a period of time, if the three way handshake has not been established between the client and Synkill, it sends a reset message to the victim server ending the connection and clears the connection from its half open connection buffer. This approach protects the victim's resource-limited half-open connection buffer from the TCP SYN attack. However, this approach requires Synkill to have more resources available than the victim to handle half-open connections. Otherwise, this approach only transfers the location and effect of the TCP SYN attack from the victim to the Synkill machine. Moreover, the potential for an attacker to exhaust the resources for established connections, at the victim, using a large number of attacking machines in a distributed attack remains.

(Malan et al. 2002) proposed "Protocol Scrubber" a scheme for removing DoS threats arising from malformed packets. Attackers may create malformed TCP packets to avoid DoS detection mechanisms designed to filter TCP traffic or exploit weaknesses in TCP implementations that lead to the victim rebooting or crashing, as in the earlier discussed Teardrop attack. The protocol scrubber is designed as a "transparent interposition mechanism for explicitly removing network attacks at both the transport and application protocol layers". The transport scrubber identifies malformed TCP packets and packets of varying TCP implementations, designed to avoid network-based intrusion detection (NID) systems or cause malicious damage. The identified packet ambiguities are removed or packets are converted to a standard TCP implementation, allowing for detection by NID systems. However, in the case of end-to-end encrypted flows, the transport scrubber assumes that the connection is sanctioned, so the protocol scrubber does not check the packet integrity.

This section has reviewed a few of the available victim based DoS defence mechanisms available. However, victim-end defences alone cannot provide complete protection from DoS attacks because victim based defences can be overwhelmed by attack traffic (Mirkovic 2003). Moreover, it is often difficult to identify legitimate traffic from attack traffic, which leads to both legitimate and attack traffic being affected by defence mechanisms. Consequently, defence

mechanisms that operate at or close to the source of the attack have emerged to distinguish between legitimate and attack traffic with a greater accuracy.

3.4.2.2 Source Based DoS Defences

There are many benefits of deploying DoS defences at or close to the sources of attacks. Defences deployed close to or on attacking zombies allow attacks to be detected before bandwidth is wasted transmitting the attack traffic from the attacker to the victim. Furthermore, dealing with a single or a few attack streams at or close to the source of the attack is considerably easier than dealing with the sum of an attack of potentially thousands of zombies at the victim end. There are few defence mechanisms currently available to defend against DoS attacks at the source of attacks. However, from the literature review, an updated list of source based defence mechanisms originally identified by (Mirkovic 2003) follows, three such defence mechanisms have been identified, Multi-Level Tree for Online Packet Statistics (MULTOPS), Reverse Firewall, and DDoS Network Attack Recognition and Defence (D-WARD).

The MULTOPS defence system consists of a tree of nodes, each of which monitors and records, incoming and outgoing, packet rate statistics for subnet prefixes at different aggregation levels (Thomer et al. 2001). These levels are compared with current packet rate statistics. If a variation between the statistical models is detected, rate limiting is applied. Consequently, MULTOPS can be implemented at the source of an attack or at the victim end of an attack. Although MULTOPS provides a valid approach for screening non-spoofed packets, MULTOPS cannot handle attack packets incorporating spoofed IP addresses. Subsequently, other methods are required to ensure incoming packets have valid IP addresses for MULTOPS to be effective. Moreover, the two-way communications statistics acted on by MULTOPS are not valid for all communication protocols. For example, certain protocols, such as UDP, may have more packets flowing in one direction.

The reverse firewall (CS3 inc 2009) resides on a personal computer or network and monitors all outgoing packets. All outgoing packets are initially permitted however only those identified to be participants in two-way

communications are permitted to transmit at high data rates. All other packets are subjected to rate limiting. This approach prevents subverted machines from launching high data rate DoS attacks. However, the reverse firewall has to maintain information on all communications. This places a large strain on the storage resources and processing capabilities of the machine hosting the reverse firewall.

D-WARD (Mirkovic 2003), operates on a router between a private network and the Internet, preventing machines on the private network from sending DoS attack packets. D-WARD analyses incoming traffic and detects DoS attacks through the detection of "non-responsive hosts" where all packets for a particular IP address are outgoing with no associated incoming packets. Additionally, ingress filtering is used to ensure all outgoing packets have valid subnet addresses, and prevent IP spoofing. Moreover, the number of outgoing connections from all of the hosts is monitored. If a significantly large number of packets are detected to originate from one particular host, a rate limit is triggered for the respective connection. Additionally, packets in a system protected by D-WARD are compared against individual models representing normal traffic flow for UDP, ICMP and TCP packet flows, increasing detection accuracy, unlike other approaches such as MULTOPS, which detect abnormal traffic using a general model for all traffic flow.

The source based DoS defences summarised in this section show that this technology offers certain advantages over more traditional victim based defences. However one significant challenge remains. DoS attacks generally affect the victim of the attack more than those closer to the source of the attack. Consequently, there is little to encourage those closer to the source of attacks to incur expenditure and install defences if they do not directly benefit. To increase the effectiveness of DoS detection and resolution further hybrid schemes have emerged which incorporate victim and source defence mechanisms.

3.4.2.3 DoS Defence - Hybrid

A number of hybrid remote DoS defence approaches have been investigated for detecting DoS attacks with a greater level of accuracy including MANAnet, Distributed Packet Filtering (DPF), Aggregate Congestion Control (ACC), Secure Overlay Service (SoS), Dynabone and the Active Security Service (ASSYST).

The MANAnet (CS3 inc 2008) approach involves creating a neighbourhood of nodes around a host, such as a web server. The neighbouring nodes stamp each packet received with a unique identifier. Once the host receives the message, the path the incoming packets have traversed from the point of entry into the neighbourhood can be identified. A fair usage policy can be implemented at the host, to provide packets from each unique path with the same level of service. This provides legitimate packets a greater share of the host's time compared to aggressive attack streams. The problem with this approach is twofold. Firstly, a fundamental change in TCP is required for the introduction of a path stamp field. Moreover, this approach works best with large neighbourhoods of nodes, ranging as close to the attacker as possible.

The DPF (Kihong et al. 2001) approach, involves filtering packets, at Internet routers, that have invalid source IP addresses. The approach is similar to conventional route-based packet filtering (RPF). However, conventional RPF requires all internet routers to install filters to be one hundred percent effective, whereas DPF requires eighteen percent coverage across Internet routers to achieve a similar effectiveness. RPF monitors the route of incoming packets at Internet routers. Using topology information the router can ascertain whether it is possible for a packet to have traversed a particular route. If it is not possible, then the packet is discarded as an attack packet. However, if an attacking host uses a spoofed IP address coming from the same route path, as the spoofed address, then the attack goes undetected. The DPF works on the presumption that there are central routers on the Internet. Consequently, locating RPFs at these locations can vastly reduce the number of nodes required to provide a similar level of defences as RPF. Moreover, in the instances where an attacker resides in the same IP neighbourhood as the spoofed IP address achieving traceback of the attacking host is simplified.

(Ratul et al. 2002) states that DoS attacks and flash crowds often overwhelm network resources and that it is not the individual packet flows which pose a problem for servers, more the aggregated effect of multiple low rate packet flows. Consequently (Ratul et al. 2002) proposes the ACC approach to identify aggregate flows causing large packet drops. Moreover, once aggregate data flows have been identified, a pushback mechanism sends a request to upstream routers to perform

rate limiting on these traffic flows. The pushback request is first sent to neighbouring routers, responsible for the aggregated traffic flow. To reduce the impact of rate limiting on legitimate traffic the routers send the pushback request further upstream, closer to the source of the attack. However, legitimate traffic is likely to be effected at the router where rate limiting is applied. This is due to the difficulty in differentiating between legitimate traffic and attack traffic destined for the same source. Moreover, this approach requires changes to routers across the Internet, to allow the pushback mechanism to be adopted. As such, it is questionable if those responsible, who do not directly benefit, will adopt this approach.

The majority of DoS defence approaches discussed and most DoS defence approaches in general are reactive defence approaches. The reactive defence approaches wait for the initiation of an attack before taking the appropriate steps to protect the victimised network (Keromytis et al. 2002). The SOS (Keromytis et al. 2002) approach, proposes the development of a proactive communication architecture more resilient to DoS attacks. The approach assumes that participants in a communication have a trusted relationship and pre-shared security material to start an authenticated session. Close to the server side of the communication or end host in peer-to-peer communications a number of firewall proxy servers, called secret servlets, form a secure overlay. The server side dynamically chooses a subset from the total number of servlets available, over which packets must travel to be accepted at the server side. Packets originating from any non-authorised servlets are immediately dropped at non-authorised intermediate secret servlets before reaching the server side destination. During a legitimate communication, clients first authenticate with a secure overlay access point (SOAP), subsequently the clients send the desired messages through the SOAP and via the secret servlets to the destination. An attacker will not know the secret servlet or combination of servlets that packets must traverse, at any one moment in time. Consequently, only packets from authenticated sources, with prior knowledge of the correct route to traverse will successfully reach the intended destination. Although an attacker may bypass the SOAP, and flood all the potential routes with attack packets, the SOS approach duplicates resources and incorporates redundancy with multiple servlets and SOAPs, significantly increasing the difficulty of conducting a flooding attack. However, the approach is only effective for nodes in a trusted relationship.

Additionally, the approach does not discuss how the trusted relationships will first be established. Moreover, the approach requires a significant amount of resource duplication, which may not be appropriate for resource-limited networks such as WSNs.

(Touch et al. 2003) proposed a variation of the SOS proactive DoS resilient communications architecture called DynaBone. The scheme proposed the deployment of multiple virtual private networks across the Internet, called layers, between trusted participants. Each layer adopts a different protocol and security mechanism, and each pair of participants has a number of layers allocated for communications. The connection bandwidth is allocated fairly between the layers. Routers along the communication path enforce the bandwidth allocation. Consequently, to launch a DoS attack an attacker has to compromise multiple layers incorporating different defence mechanisms. However, for DynaBone to be effective all routers along the communication path, between communicating parties, must adopt the DynaBone system and support bandwidth allocation based on layers. Moreover, routers adopting the DynaBone approach must enforce all connecting clients to use the DynaBone approach, or the routers must reserve a portion of bandwidth for the DynaBone system and a portion of bandwidth for normal Internet traffic. Otherwise, an attacker may flood a router with normal attack traffic and prevent traffic from the DynaBone virtual private network/layers from reaching the router. Consequently, the extensive infrastructure changes required by the DynaBone approach make such a system impractical. Moreover, although DynaBone is deployed across the infrastructure of the Internet, the approach requires the end network to support all of the security mechanisms employed by the different layers, this makes such a system impractical for low cost, resource limited WSNs.

(Cotroneo et al. 2002) proposes ASSYST, a distributed DoS defence system incorporating network routers, and a bespoke Active Security Protocol (ACP). The primary role of the ACP protocol is to help nodes share DoS attack information with neighbouring nodes. During an attack, any router that first detects an attack sends an alert message using ACP, containing information about the attack characteristics to neighbouring routers. The neighbouring routers use the information received to

detect if the attack exists in their region, if the attack characteristics are detected a response message is sent back to the first router to detect the attack. Consequently, using the feedback from upstream routers, the initial router to detect the attack calculates the path of the attack from source to end. This allows the initial router, at the start of an attack path, to pick the optimum response and send an instruction to the appropriate routers informing them of the action to take. The novel traceback mechanism provides an effective method for identifying the path of attacks. However, the approach requires the modification of all routers on the Internet to be fully effective. Moreover, for every attack a router detects a flood of messages is sent across neighbouring nodes to perform an analysis of DoS activity in their respective regions. Consequently, an intelligent attacker may launch a fake DoS attack in order to make the routers flood the network with analysis request messages.

Hybrid remote DoS defence approaches allow for the traceback of attacks close to the source. Consequently, attack traffic can be more accurately filtered close to the source of attacks, leading to less of an impact on legitimate traffic. Moreover, mitigation of attacks close to the source of attack traffic requires defences with fewer resources, opposed to further upstream where tackling the aggregated attack traffic from multiple hosts requires defences with much greater resources to prevent being overwhelmed by attack traffic. Conversely, the hybrid approaches allow attacks to be detected upstream where the aggregated effect of attack traffic is more evident. The greatest difficulty that arises in adopting hybrid DoS defences is in creating consensus and enforcing the worldwide implementation of a standard for the creation of interoperable source and victim end defences (Mirkovic 2003). Although, the Internet has seen the adoption of worldwide standards before, it is questionable if users who do not directly benefit from DoS defences will or should pay the added cost of adopting such technology.

3.5 Conclusions

This chapter has provided a comprehensive review of the threats faced by WSNs from DoS threats originating from within WSNs (local attacks) and from neighbouring networks (remote attacks). The objective of both local and remote attacks is to prevent WSNs from providing services to legitimate users.

The local DoS threats that originate from within WSNs have been classified based on the layer of the WSN protocol stack targeted by the attack. There is a considerable amount of research available on DoS attacks and defences for threats that originate from within WSNs (Raymond et al. 2008) and (Wood et al. 2002), see Table 3-1. The existing defences overcome most of the attacks identified through a combination of resource duplication, and cryptographic techniques used to authenticate packets, verify the integrity of packets, and prevent the replay of packets (Raymond et al. 2008). However, from the literature reviewed. there is little research available on the effects of DoS attacks launched from subverted nodes, which have access to cryptographic material used by the existing DoS prevention mechanisms.

The DoS threats that originate from outside WSNs and target the WSN directly or target the remote access infrastructure of the WSN have been classified based on the approaches that take a brute force approach and those that exploit vulnerabilities (Mirkovic et al. 2004). The brute force based attacks attempt to overwhelm the resources of a victim used to provide services. Consequently, during a DoS attack legitimate users are prevented from accessing service because there are insufficient resources available to handle their requests. The vulnerability based DoS attacks, target flaws in the software implementation of systems to cause the service offered by the victim to be degraded or altogether stopped. There is a great deal of research available regarding the effects of remote DoS attacks against enterprise servers, however from this review, and as identified by (Kumar et al. 2006), there is little research regarding the effect of these attacks on WSNs.

Table 3-2: Comparative analysis of DoS defence tools.

DoS Defence	Percentage of DoS attack packets removed
D-WARD	99.4%
Aggregate Congestion Control (ACC)	64.0%
ASSYST	89.2%
MULTOPS	93.0%

The DoS defences that attempt to resolve these remote DoS threats have been classified based on the location of their implementation, including those implemented at the victim-end, source-end, and hybrid schemes located at both the

victim-end and source-end of attacks (Mirkovic et al. 2004). The proposed DoS defence approaches, targeted at defending against DoS flooding attacks, do not consistently provide a statistical summary of the percentage of DoS attack packets detected and removed. However, from the literature review, the proposed effectiveness of certain DoS defences, where stated or possible to derive is summarised in Table 3-2 from (Mirkovic et al. 2004), (Ratul et al. 2002), (Cotroneo et al. 2002), and (Thomer et al. 2001). As highlighted in Table 3-2, the D-WARD attack tool, is the most effective DoS defence identified from the literature review, removing 99.4% of attack traffic. Consequently, it is used as the benchmark approach to evaluate the proposed defence approaches, in the following Chapters. As with the research on the effectiveness of DoS attacks against WSNs, there is little research available on the appropriateness of these defences for protecting WSNs, which have significantly fewer resources available than conventional servers (Perrig et al. 2004) & (Kumar et al. 2006). Consequently, in Chapter 7 the D-WARD approach is used to evaluate the effectiveness of the defence with the highest identified effectiveness of combating DoS flooding attacks targeted at WSN's and as a benchmark to evaluate the proposed defence approaches.

Chapter 4

Research Methodology

4.1 Introduction

This chapter provides an overview of the research methodology adopted for the research and the rationale behind the adopted methodology, followed by a detailed description of the research undertaken at different stages of the research methodology.

4.2 Adopted Research Methodology

The objectives of this research require the use of both quantitative and qualitative approaches. The research project involves the analysis of existing DoS attacks on resource limited WSNs and the evaluation of existing defences, both to confirm limitation of the existing defences identified from the domain analysis and as a benchmark to gauge the relative effectiveness of the new proposed approaches. This was accomplished using quantitative strategies such as design, implementation and experimental evaluation of the existing and proposed DoS defence approaches. The quantitative approaches help to provide statistics such as, the percentage of an attack mitigated by an existing DoS attack, for providing a benchmark to contrast the improvement of the proposed approaches. However, the effectiveness of a DoS defence is largely based on the user's perceptions of if they are receiving an

acceptable level of service during a DoS attack. Consequently, to evaluate the effectiveness of the existing and proposed approaches, a qualitative approach is also required. Consequently, the systems development methodology was adopted for the research, due to its incorporation of both the quantitative and qualitative approaches, as required by the research objectives. There are more than twenty different systems development methodologies (Avison & Fitzgerald 2003), a review of these methodologies is outside the scope of this thesis. However, as identified by (Burstein 2002), all of these methodologies recognise three main stages consisting of a concept development stage, system building stage, and an evaluation stage. Moreover, these stages do not necessarily follow a linear pattern, certain stages can be repeated and revisited and other stages can sometimes be omitted, for example, the concept development stage may be revisited during the systems building stage (Hasan 2004). These stages were adopted as components of the system development methodology. A brief summary of these stages is provided in Table 4.1, followed by a thorough discussion of the research undertaken at each stage.

Table 4.1 Systems development methodology stages and research undertaken

Stage	Research Undertaken
Concept Development	Investigation and Domain Analysis • Literature Review • Identification of potential DoS weaknesses in WSN based HASs and the existing DoS defences
Systems Building	Design of a WSN based HAS test-bed • Design of a WSN based HAS • Development of a WSN based HAS • Unit Testing • System Testing of WSN based HAS Development of the dominant remote access approach "GHS" (see Chapters 2 & 6 for more information), as a benchmark for evaluating the proposed approaches

	Design of a hybrid communication approach based DoS defence against third party DoS attacks • Design of third party DoS defence • Development of third party DoS defence • Unit testing • System testing of third party DoS defence, against the benchmark GHS approach Development of the most effective existing DoS defence for flooding DoS attacks directly against a network "D-WARD" (see Chapters 2 & 7 for more information), as a benchmark for evaluating the proposed approaches Design of a hybrid communication approach based DoS defence against direct DoS flooding attacks and attacks targeted at the home gateway. • System design of a DoS defence against flooding attacks and home gateway attacks • Development of defence against flooding attacks and home gateway attacks • Unit Testing • System Testing of DoS flooding and gateway attack defences, against the benchmark D-WARD approach
Systems Evaluation	Evaluation • Home automation test-bed evaluation • Evaluation of the proposed DoS defences

4.2.1 Concept Development Stage

The concept development stage consisted of an extensive literature review. As part of the literature review, the existing WSN based HASs were investigated and analysed to assist in the development of a WSN based HAS test-bed. Moreover,

a thorough review of the existing DoS attacks and defences was undertaken. The review allowed the existing knowledge on DoS attacks and defences to be applied to WSN based HASs to identify potential threats from DoS attacks, identify the limitations of the current defences for protecting WSN based HASs, and assist in the development of research objectives.

4.2.2 System Building Stage

The system building stage consisted of three phases. During the first phase a WSN based HAS test-bed was designed, developed, and tested. The test-bed was developed as part of a much larger industry sponsored project, the project and relevant contributions are discussed further in Chapter 5. From the literature review, it can be concluded that the majority of research into DoS attack on WSN based HASs is based on simulation studies. The test-bed allows for the first experimental evaluation of existing DoS attacks and defences on a resource limited WSN based HAS. Consequently, contributing to the available knowledge on DoS attacks against WSN based HAS from a different perspective. The test-bed was developed in parallel to the DoS defences designed and developed during the second and third phase. The period during which the WSN based HAS was developed, in relation to phase two and three, was specified by the project's industrial partners. Consequently, the timing of the first phase in parallel to the second and third phases was not based on the researcher's criteria. Although, this imposed some limitations on the hardware adopted for the DoS defences in phase two and three, this was considered an acceptable compromise due to the added benefit of testing the proposed approaches with a working WSN based HAS, as discussed earlier.

During stage two, the existing dominant remote access approach (GHS) identified from the literature review, see Chapter 2, was implemented on the WSN based HAS test-bed, to provide a benchmark for the proposed approaches. Moreover, a hybrid communication approach for increasing the DoS resistance of a third party, mediating communications between remote users and a WSN based HAS, was proposed. Initially, based on the earlier discussed domain analysis, a conceptual model of a hybrid communication approach to defend against DoS attacks was proposed (see Chapter 6, Figure 6-2 and 6-3). Based on the conceptual model a remote client, remote home server (trusted third party), and home gateway

were developed, as a proof of concept, to demonstrate that such a hybrid communication approach is viable. The home gateway was developed as part of phase one, however was influenced by the conceptual model designed during the parallel phase two. Initially, a personal computer functioned as the home gateway, as illustrated in (Gill 2008b). Once the conceptual model had been tested on the personal computer based home gateway, an embedded home gateway was developed and integrated with the WSN based HAS, as introduced in Chapter 6 and 7. Unit testing of the RHS-1 and RHS-2 communications approaches was conducted before the approaches were combined to form the hybrid communications approach. Next, the hybrid communications approach was integrated with the WSN based HAS test-bed, alongside an existing remote access approach GHS, discussed in Chapter 6, to provide a benchmark for the proposed approach. The GHS benchmark is dependent on the hardware used. Consequently, the GHS is implemented on the test-bed, and a benchmark calculated (see Chapter 6 for more details). The test-bed was subjected to a DoS attack and the performance of the proposed approach was compared against the benchmark approach.

During phase three, the most effective existing DoS defences "D-WARD" identified from the literature review, see Chapter 3, that claims to prevent 99.4% of attack packets was implemented on the WSN based HAS test-bed, to provide a benchmark for the proposed approaches. Moreover, a hybrid communication approach for increasing the resistance of WSN based HASs to flooding and home gateway DoS attacks, was proposed. As before, the initial stage involved the creation of a conceptual model of the hybrid communication approach, based on the earlier domain analysis. The next stage required the development of a virtual home and DDoS Defence Server as part of the hybrid communication approach. Moreover, the RHS-1 and RHS-2 communication approaches developed as part of phase two, were also adopted for the hybrid communication approach in phase three. Alongside the proposed hybrid communication approach, a model of the most effective DoS attack identified from the research "D-WARD" was also developed to provide a benchmark to both analyse the effectiveness of existing defences and provide a relative comparison of the performance of the proposed approach. Additionally, a DoS attack tool was developed to launch an application level DoS flooding attack against the WSN based HAS and the home gateway. The proposed

hybrid communication approach was integrated with the WSN based HAS. For the evaluation of the proposed hybrid communication approach a DoS attack was launched from the attack tool, against the test-bed with only the existing defences in place, to create the benchmark to evaluate the proposed defences. Next, the experiment was repeated with the existing defences and the virtual home in place to evaluate the effectiveness of the virtual home at protecting WSN based HASs from flooding DoS attacks. Then the experiment was repeated with the existing defences, virtual home and DDS in place to evaluate the effectiveness of the DDS to work in unison with the virtual home and protect WSN based HASs from DoS attacks against the home gateway.

4.2.3 System Evaluation Stage

During the system evaluation stage, the system is tested as a whole. During this stage, the validity of the WSN based HAS as a test-bed was investigated. A field trial was conducted where the WSN based HAS was used by a potential user in their home for a period of twelve days, after which the homeowner completed a questionnaire to identify how the system functioned and highlight any issues. An email was sent out to potential homeowners at Loughborough University and amongst staff at one of the projects industrial partners. This resulted in one family volunteering to take part in the field trial. Due to the limited number of participants available for the field trial, a focus group was held where potential homeowners were shown the system and asked to complete a questionnaire. Next, the proposed hybrid communication approaches, discussed during the system building stage, were evaluated to establish the approaches functionality, robustness, and ease of use through a focus group session of potential home occupiers at east midlands airport. During the focus group, participants were introduced to the WSN based HAS test-bed and shown the effects of a flooding DoS attack against the third party, WSN based HAS and home gateway with only the existing defences in place and the effect of the same attack with the proposed defence mechanisms in place. At the end of the demonstration, the participants were asked to complete a questionnaire. Additionally, a questionnaire was conducted to identify any human computer interaction factors that might affect the proposed DoS defence approaches. The

questionnaire was conducted amongst the first set of participants which evaluated the WSN based HAS, due to their familiarity with WSN based HASs.

4.3 Summary

The chapter has introduced the systems development methodology and justified the adoption of this methodology. Additionally, the stages of the methodology and the respective research undertaken at each stage have been discussed and highlighted in Table 4.1. Moreover, the existing approaches (GHS, and D-WARD) used as benchmarks to evaluate the effectiveness of the proposed approaches have been highlighted.

Chapter 5

Design of a Home Automation Test-Bed

5.1 Background and Motivation

As identified from the literature review (see Chapter 3) the majority of existing research into DoS attacks and the design of defence measures focuses on theoretical studies using simulations. Although, simulation oriented research provides a valid analysis of proposed ideas, simulations do not take into consideration all of the factors associated with implementing approaches in the real world, including environmental factors that may inadvertently affect proposed approaches. As such, simulation studies alone are not sufficient to evaluate the efficiency and effectiveness of DoS defence approaches to meet the requirements of specific applications, placed under the strain of normal usage, in a real environment. Consequently, the research presented in the following chapters provides the first evaluation of DoS vulnerabilities in WSN based HASs and the effectiveness of the proposed defence approaches, through a series of experiments on a real home automation test-bed. Although as with simulation studies, experimental studies have their own limitations (Bausell 1986), they provide a means to analyse the affects of DoS attacks on WSN based HASs from a different perspective to the existing research. The home automation test-bed design is based on the current trends in research identified from the literature review. Moreover, the test-bed communications architecture is based on the ZigBee standard, one of the latest

standards developed for low cost, wireless home automation (Barontib et al. 2007). This chapter presents the development of a ZigBee based HAS test-bed. The test-bed is used to quantitatively evaluate the vulnerability of such systems to flooding DoS threats, in the following chapters. Moreover, the existing dominant approaches for remotely communicating with WSN based HASs (Direct and GHS, see Chapter 6) and the existing DoS defences (D-WARD, see Chapter 7) are integrated with the test-bed as benchmarks to evaluate the proposed DoS defence approaches, in the following chapters. This chapter provides the details required to reproduce the WSN based HAS test-bed, to reproduce the experiments in the following chapters. The work presented in this chapter is published in (Gill et al. 2009a), (Gill et al. 2007), and (Yao et al. 2007).

5.2 Analysis of the Existing Systems

The adoption of home automation technology by consumers has been limited. We propose that, from the home automation domain analysis, the problems limiting wide spread consumer adoption can be grouped into five general categories. Firstly, ***complex and expensive architecture***: the existing systems architectures generally incorporate a personal computer for the purposes of network management and provision of remote access. This adds additional complexity to the system, hence increasing the overall fiscal expense. Secondly, ***intrusive installation***: the majority of systems require varying levels of physical wiring in their architectures. This, in some cases, is due to the expense of the alternative wireless technologies. Hence, these systems require intrusive and expensive installations. Thirdly, ***lack of network interoperability:*** both home networks and the HASs which utilise them have been developed and adopted in an unplanned and ad hoc manner. This has lead to a home environment consisting of a complex maze of heterogeneous networks. These networks and the systems that utilise them normally offer little interoperability; leading to three potential problems

- duplication of monitoring activities, due to lack of interoperability,
- the possibility of interference, between coexisting networks, and

- the potential for two simultaneous, autonomous actions on coexisting networks, interacting and resulting in an undesirable outcome.

Fourthly, ***interface inflexibility***: the existing systems offer varying approaches for users to control and monitor the connected devices. However, this is normally limited to a single method of control, which offers users limited flexibility. The systems that provide more than one interface device normally provide different user interfaces and risk confusing users. Finally, ***security and safety***: the existing approaches have not focused on security and safety problems that may arise from their implementation. Moreover, the systems that offer some degree of security have neglected the problems with sharing information between devices produced by multiple vendors for the purposes of establishing security.

5.3 Features of the Proposed System

The architecture of the home automation test-bed is designed to reduce the system's complexity and lower fiscal costs. Hence, the system endeavours not to incorporate complex and expensive components, such as high-end personal computers. The system is flexible and scalable, allowing additional home appliances designed by multiple vendors, to be securely and safely added to the home network with the minimum amount of effort. The system allows homeowners to monitor and control connected devices in the home, through a variety of controls, including a ZigBee based remote control, and any Wi-Fi enabled device that supports Java. Additionally, users may remotely monitor and control their home devices using any Internet enabled device with Java support. Moreover, a home gateway is implemented to facilitate interoperability between heterogeneous networks and provide a consistent interface, regardless of the accessing device. Furthermore, a virtual home pre-processes all communications before they are realised on the real HAS, ensuring all communications are checked for security and safety before being allowed to continue to their respective destinations.

5.4 System Architecture

The home automation test-bed adopts two wireless standards to cater for the low and high rate communication needs of users. The low data rate, control and

monitoring needs are catered for using Zigbee and the test-bed's high data rate needs, such as multimedia applications, are met by the Wi-Fi (IEEE 802.11g) standard.

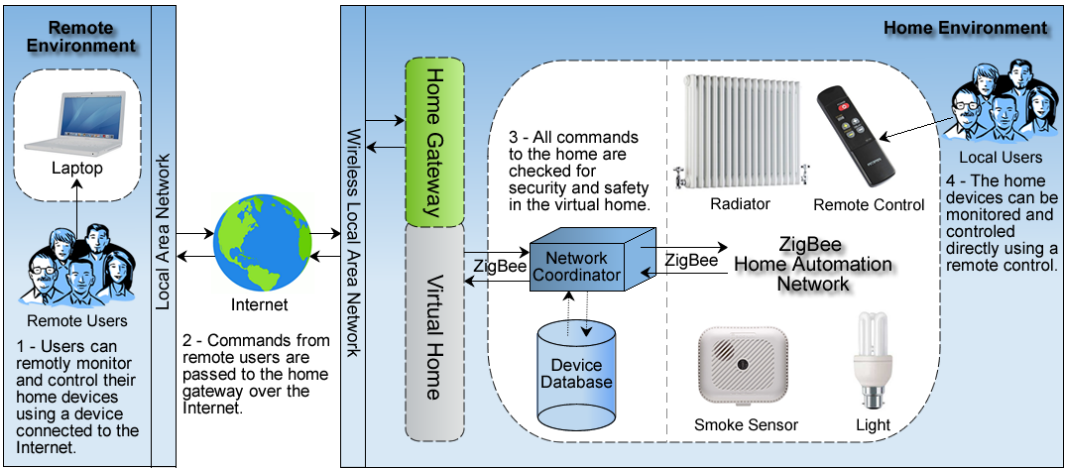

Figure 5-1: Conceptual architecture overview of home automation test-bed (Gill et al. 2009a)

A home gateway is implemented to provide interoperability between the heterogeneous Zigbee and Wi-Fi networks, and facilitate local and remote, control and monitoring of the home's devices. A virtual home is implemented for the provision of real-time security and safety for the home and its inhabitants.

As depicted in Figure 5-1, the proposed system consists primarily of four interconnections. Remote user can access the system using the Internet. The remote user's communications traverse the Internet until they reach the home network. Communications are then wirelessly transmitted to the Home Gateway using the homes Wi-Fi network. The Home Gateway hosts the virtual home, which checks and processes all communications, as discussed later. Once checked the communications are sent to the real HAS and the respective device. Additionally, a local ZigBee based remote control allows direct control over connected devices.

5.4.1 Residential Networks

As discussed, the proposed system architecture implements a ZigBee based home automation network and a Wi-Fi based multimedia network. Alternative standards could have been integrated with the home gateway. However, the use of Zigbee and Wi-Fi offers certain advantages. As discussed in Chapter 2, Zigbee technology is designed for applications that require low data rate, low-cost, low

power consumption, and two-way wireless communications. The Wi-Fi standard is designed to provide relatively high data rate communications. Wi-Fi has the advantage of an existing and wide spread presence in homes in the United Kingdom. The combination of Zigbee and Wi-Fi technologies has the potential to provide a comprehensive home automation solution.

5.4.2 Zigbee technology

As discussed in Chapter 2, ZigBee is a RF communications standard based on IEEE 802.15.4. Figure 5-2 depicts the general architecture of a Zigbee based home automation network. The Zigbee coordinator is responsible for creating and maintaining the network. Each electronic device (i.e. Washing Machine, Television, Lamp etc) in the system is a Zigbee device managed by the coordinator. All communication between devices propagates through the coordinator to the destination device. The wireless nature of ZigBee helps overcome the intrusive installation problem with the existing HASs identified earlier. The ZigBee standard theoretically provides a data rate of 250kbps, which is sufficient for controlling most home automation devices. The low installation and running cost offered by ZigBee helps tackle the expensive and complex architecture problems with existing HASs, as identified earlier.

5.4.3 Wi-Fi Technology

In the proposed system architecture, Wi-Fi is used for two primary purposes. Firstly, it is the chosen communication standard for multimedia applications in the home. Secondly, it is used to provide access to the home's HAS from Wi-Fi enabled devices, as an alternative to the Zigbee based local controller. This approach is taken because, as discussed in Chapter 2, homes increasingly have Wi-Fi networks and Wi-Fi enabled devices such as PDA's and mobile phones. The additional cost of a Zigbee based controller in these situations is unwarranted. Moreover, the high data rate nature of Wi-Fi allows for greater flexibility in interface design. Wi-Fi implements the IEEE 802.11 standard and offers wireless networking using RF communications. There are different versions of the 802.11 protocol. The dominant protocol in use today is IEEE 802.11g, which operates in the unlicensed 2.4 GHz band and provides a maximum data rate of 54 Mbps.

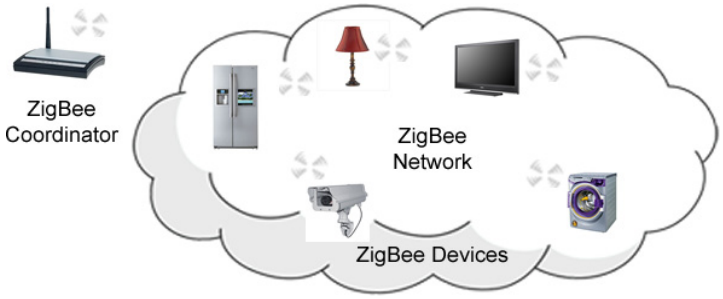

Figure 5-2: A generic Zigbee home automation architecture

The use of Wi-Fi offers several advantages over alternative technologies. The Wi-Fi standard is more established in homes in the UK than alternatives such as Bluetooth, as a wireless home networking technology. The result is less equipment expense for the consumer, and the use of a familiar technology.

5.4.4 Network Coexistence

Heterogeneous and homogenous home networks may coexist with each other in the same environment. The problem of interference between these networks increases as more and more standards emerge which use the same communication medium. Technologies such as Bluetooth, microwave ovens and cordless telephones can cause interference with Zigbee. However, Zigbee and Wi-Fi can exist together with less interference problems than alternative technologies currently available (Shuaib et al. 2006), hence offering the best combination available for the home automation test-bed.

5.4.5 Home Gateway

The home gateway, as depicted in Figure 5-1, is charged with providing interoperability between different connecting networks. The home gateway provides two primary functions for the proposed architecture. Firstly, the home gateway provides data translation services between the Internet, Wi-Fi, and ZigBee networks. Secondly, the home gateway provides a standardised user interface for devices connecting to the ZigBee home network, remotely using the Internet or locally using the Wi-Fi network. The home gateway does not provide a standardised interface for the local ZigBee remote control. This decision was made to allow greater freedom for interface design and avoid limitations that have to be taken into consideration for the design of the low data rate, low power ZigBee remote control

interface. Although, as depicted in Figure 5-1, the close cooperation between the home gateway and device database allows for the real-time control and monitoring of all home devices, regardless of the access device and network used. The home gateway is implemented as part of the proposed HAS's architecture to overcome the problem of insufficient network interoperability, identified in existing home automation approaches. Moreover, the proposed approach looks at the existing network structure within the home environment and integrates predominantly established networks in the existing home environment. Additionally, the home gateway reduces the inflexibility in the control modes of existing HASs, through the prevision of manual, local and remote control. Furthermore, the interface of the controlling devices is standardised across the control modes.

5.4.6 Virtual Home

The virtual home, as depicted in Figure 5-1, is responsible for the administration of security and safety for the HAS. The virtual home, as the name suggests, is a virtual environment where the actions requested by users are checked. For the purposes of security, all the messages received by the virtual home are checked by authenticating the sender, checking the integrity of the messages to prevent tampering, and protecting the confidentiality of messages through the use of encryption. The system's safety is protected by ensuring the commands received are appropriate for the respective home network and that all changes requested fall within the specified safety limits. The primary objective of the virtual home is to prevent any event that may pose a security or safety concern from implementation on the home automation test-bed. A virtual home, incorporating a simple encryption mechanism for providing protection for communications integrity and confidentiality, was introduced during the development of the test-bed. The development of the virtual home allows the feasibility of the virtual home concept and positioning of the virtual home to be evaluated before the test-bed is used in experiments and subjected to DoS attacks with and without the novel DoS defence mechanisms developed and discussed in later chapters.

5.4.7 Device Engine

The HAS is designed to be flexible, allowing different devices designed by multiple vendors to be connected. Consequently, each device incorporates a dedicated engine, responsible for providing the necessary application functionality and ZigBee network connectivity. Moreover, each device engine may contain dedicated security and safety measures. Furthermore, the device engine has code to facilitate the collaboration of the devices with the virtual home.

5.5 Home Automation Test-Bed Implementation

The proposed HAS test-bed was developed and implemented as part of a much larger TSB (Technology Strategy Board) funded project called "indeedNET" (Integration and demonstration of energy efficient dwelling networks) (indeedNET 2007). The author is a member of the team which designed and developed the HAS test-bed. In particular, the authors contributions focused on the design of the HAS architecture, initial development of a prototype home gateway, software development for the home gateway including development of the virtual home, and evaluation of the HAS test-bed. Other members of the indeedNET team are responsible for developing the hardware aspects of the HAS test-bed such as the creation and evaluation of the end devices discussed in the following section, the underlying network infrastructure, and development of the final version of the home gateway, as depicted in Figure 5-3. The overall development of the HAS test-bed discussed in the remainder of this chapter, consists of the authors and colleagues contributions. The overall development is reviewed in order to provide the readers with a comprehensive understanding of the HAS test-bed used for the evaluation of existing and proposed approaches for enhancing the security of WSN based HASs in the remainder of the thesis. The source code of the WSN based HAS test-bed is provided in Appendix C. The source code, together with the information provided in this chapter, allows for the WSN based HAS test-bed described in this chapter and used to evaluate the proposed DoS defences, introduced in the following chapters, to be reproduced. It should be noted that the source code is provided for the purpose of repeatability of the research included in this Thesis. The code is developed as part of the indeedNET project, and as such is the contribution of a team of people, of which the author is a member.

The implementation of the proposed system is illustrated in Figure 5-3. As depicted, a ZigBee based HAS test-bed is implemented for the monitoring and control of household devices. To cater for the household's high data rate needs, such as multimedia entertainment, a Wi-Fi network is implemented. A home gateway has been developed to provide interoperability between these networks. The home gateway presents a unified interface for users to locally and remotely access home networks. The security and safety of the home automation network is realised through the development of the earlier described virtual home on the Home Gateway. To demonstrate the feasibility and effectiveness of the proposed test-bed four devices, a light switch, radiator valve, safety sensor and ZigBee remote control have been developed and integrated with the test-bed.

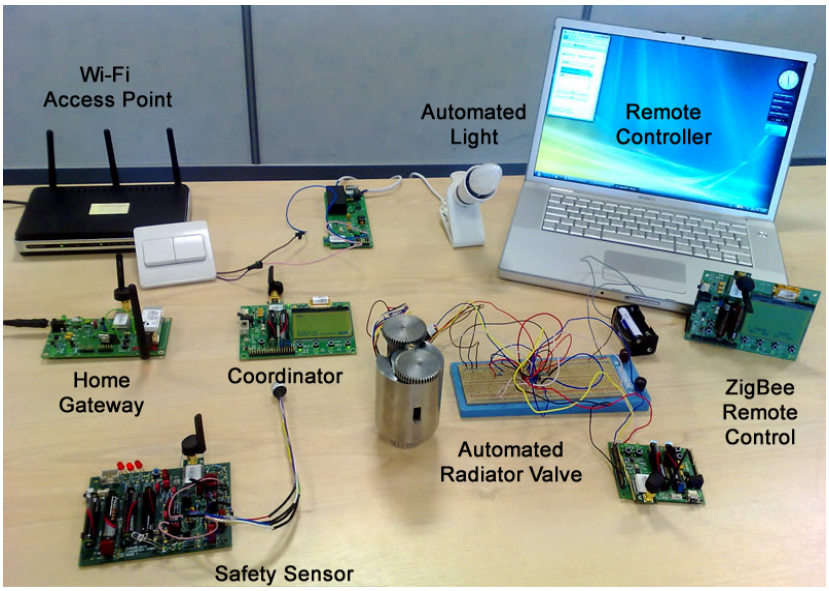

Figure 5-3: Home automation Test-Bed implementation

5.5.1 ZigBee Home Automation Network

The ZigBee home automation network consists of a coordinator, routers and several end devices. The coordinator is responsible for starting the ZigBee network. During the network initialisation phase, the coordinator scans the available radio channels to find the most suitable one. Normally this will be the channel with the least activity, in order to reduce the level of interference. It is possible to limit the channels scanned, for example excluding those frequencies ranges used by the Wi-Fi network included in the proposed architecture. However, our experiments have shown that the average time taken (to the nearest second) to scan all the available

channels is 9 seconds. This scan time is relatively small and as the home coordinator is initialised infrequently this is an acceptable delay when contrasted with the performance increase possible through the use of a channel with less interference. The coordinator is pre-programmed with the PAN ID (Personal Area Network Identifier), although it is possible for the coordinator to dynamically scan for existing network PAN IDs in the same frequency and generate a PAN ID that does not conflict. All home devices connected to the ZigBee home automation network are assigned a fixed 64 bit MAC address. Additionally, each device is assigned a dynamic 16 bit short address that is fixed for the lifetime of the network. At this stage of the network initialisation, the coordinator assigns itself the short address 0x0000. After the coordinator's initialisation phase the coordinator enters "coordinator mode", during this phase it awaits requests from ZigBee devices to join the network.

The ZigBee devices developed for the home network, as mentioned, includes a light switch, radiator valve, safety sensor and ZigBee remote control. A ZigBee end node has been integrated with these devices. As the devices are started, during their respective initialisation stage, the node scans for available channels to identify the network it wishes to join. There may be multiple networks in the same channel, these networks are normally distinguished by their PAN ID. The node selects which network to join based on the PAN ID. The node sends a request to the network coordinator to join the network. The request is sent to the coordinator directly or through a neighbouring router on the desired network with which the node shares the best signal. On receipt of the request, the coordinator judges whether the requesting device is permitted to connect to the home automation network. The standard implementation of most ZigBee networks prevents unauthorised devices joining the network by providing a short user defined period when devices may join. This does not provide sufficient network security. To enhance the system's security the proposed system encrypts all device communications including the requests to join the home network with a private key. Only those devices that are in possession of the correct private key can successfully connect to the home network. The devices that are permitted to join the network are recorded in the device database and stored on the network coordinator. A partially connected mesh topology was adopted for the ZigBee home automation network.

Due to the nature of the home environment where communication interference is constantly fluctuating, the advantage of increased communication routes available through the adoption of a partially connected mesh topology outweighs the added routing complexity. The ZigBee coordinator and end devices are composed of an off-the-shelf Jennic 5139 modules (Jennic 2009), the code required in addition to the previous architecture and description is available in Appendix C.

5.5.2 Wi-Fi Network

The homes Wi-Fi network is implemented through a standard Wireless (802.11b and 802.11g) ADSL Modem Router, with a 4 port switch. The modem provides two primary functions. Firstly, the modem provides the connection between the Internet and local Wi-Fi network; hence extending access to the Wi-Fi enabled home gateway to any location with Internet access. Secondly, any local Wi-Fi enabled device within range of the home's Wi-Fi network can directly access the home gateway. This provides a low cost communication method with the home network, and reduced infrastructure costs where Wi-Fi devices are already in use. The Wi-Fi network was created using no security and a SSID of "home".

5.5.3 Home Gateway

A thorough review of existing home gateway technologies revealed that no off-the-shelf solution exists that provides the functionality specified in the requirements for the home gateway. This included the provision of interoperability between the Internet, Wi-Fi and ZigBee networks. Consequently, a PC based home gateway was initially developed, as discussed in (Gill et al. 2008b). Once the concept of the home gateway had been tested, a bespoke home gateway, as shown in Figure 5-4 was developed. The home gateway consists of a Wi-Fi module, a ZigBee node and a power supply. The Wi-Fi module provides low cost, embedded Wi-Fi connectivity. The ZigBee microcontroller provides the connection to the ZigBee network. The Wi-Fi module connects to the home's local Wi-Fi network and the ZigBee microcontroller connects to the ZigBee home network as an end device. The home gateway once started enters the configuration stage. During the configuration stage the embedded Wi-Fi module establishes a connection with a local Wi-Fi network.

The parameters for the Wi-Fi connection such as network SSID and security parameters are preconfigured. Simultaneously, the ZigBee microcontroller searches for a ZigBee home network and, as discussed, establishes a connection. As with the Wi-Fi module, the ZigBee microcontroller's connection parameters are preconfigured. This concludes the configuration stage.

Figure 5-4: Home gateway

Once the home gateway has been initialised, an idle state is entered into until input is received. Input can originate from both the Wi-Fi network for input to the ZigBee network, or conversely from the ZigBee network for output to the Wi-Fi network. Input from the Wi-Fi network normally takes the form of commands from user interface devices. The input from the ZigBee network normally takes the form of responses to commands received earlier from user interface devices. The ZigBee node was an off-the-shelf Jennic JN5139 node (Jennic 2009), the Wi-Fi module was an off-the-shelf Digi Wi-Fi module development kit (Digi 2009). The development kit allowed the interconnection of the Jennic JN5139 module with the Digi Wi-Fi module using a serial connection. The Digi Wi-Fi module comes preconfigured with firmware, the only configuration required was to set the Wi-Fi module SSID to "home" to allow the module to connect with the local Wi-Fi connection. The software required to make the Jennic JN5139 module operate is included in Appendix C.

5.5.4 Virtual Home

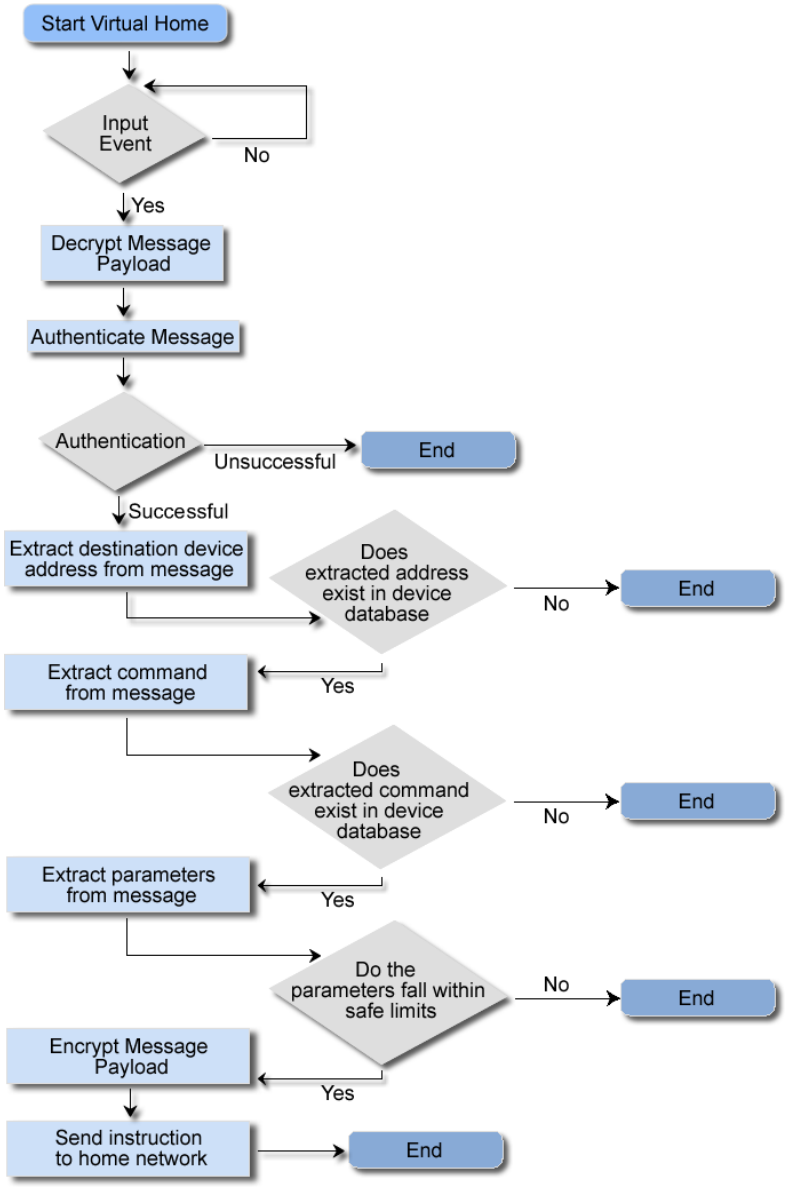

Figure 5-5: Virtual home flow chart

The virtual home is a software construct developed in C. The virtual home is implemented on the home gateway. All communication and instructions are checked, as illustrated in Figure 5-5, for security and safety, in the virtual environment, before implementation in the real home environment. The virtual home waits for input from an external source. All devices on the ZigBee network incorporate the ZigBee microcontroller and a dedicated AES coprocessor. Sensitive communications on the home network are encrypted. Hence, the message payload of sensitive communications received by the virtual home from legitimate sources will be encrypted with a valid symmetric key. Once the authenticity and integrity of

messages has been established, the virtual home checks the safety implications of the messages. After decryption, the destination device address is extracted from the message and checked in the device database for its existence. Once the device's existence on the network has been established, the command and parameters included in the message are extracted. The existence of the command for the respective device is checked to ensure the real device offers the requested functionality. The extracted parameters are compared against predefined safe ranges for the respective device and command. Only after the message has been processed by the virtual home algorithm for security and safety and declared safe is the message re-encrypted and forwarded to the real home network device. The virtual home is modified in the following chapters, before the evaluation of existing and proposed DoS defences with the WSN based HAS test-bed. Consequently, the pseudo code of the virtual home is given after modifications in Chapter 7.

5.5.5 User Interface Devices

To evaluate the effectiveness of the system architecture for the provision of easy to implement, and flexible modes of control; three control modes were developed.

ZigBee Remote Control: A low cost, simple-to-use remote controller, for the local monitoring and control of devices was developed. The controller board consists of a ZigBee JN5139 node with an LCD display, and four push button switches and is powered by four AA batteries (Jennic 2009). Instructions from the remote control traverse the home network until received by the destination device.

Remote Access Device and Wi-Fi Remote Control: A standard mobile phone (Nokia N95) with built in support for Wi-Fi and J2ME is used to access and control the system. While locally accessing the system the mobile uses Wi-Fi to freely access and control the system. When a Wi-Fi connection is not available, the mobile establishes an Internet connection to access and control the system. In both scenarios, the instructions sent from the mobile phone are received by the home gateway, which translates the communication and forwards it to the virtual home, as discussed, before being sent to the destination device. The development of the

software for the mobile phone is discussed in Chapter 6, and the software code is provided in Appendix D.

5.5.6 Home Automation Devices

To demonstrate the feasibility and effectiveness of the proposed test-bed three devices; a light switch, radiator valve, and safety sensor, are developed. These devices are depicted in Figures 5-6 (a), (b), and (c) respectively.

a. b. c.

Figure 5-6: (a) ZigBee operated light bulb in the off state; (b) ZigBee based automatic radiator valve; (c) ZigBee safety sensor

Light Switch: A conventional light switch is integrated with a ZigBee microcontroller, as shown in Figure 5-6 (a). In this prototype the user accesses the light switch, detect the lights current state ("On" or "Off"), and adjust the state accordingly.

Radiator Valve: A prototype automatic radiator valve is developed and integrated with a ZigBee microcontroller, as shown in Figure 5-6 (b). The valve can be manually controlled, as are conventional valves, and remotely monitored and controlled.

Safety Sensor: The safety sensor has special characteristics of interest. For instance, unlike most devices, the safety sensor has to continuously monitor its environment and provide feedback. This reduces the time the device can operate in sleep mode, hence considerably reducing the battery life. A safety sensor is developed (see Figure 5-6 (c)) to investigate the potential viability of the HAS test-bed with a mass-market end device that places a large demand on system resources. The safety sensor incorporates temperature, carbon monoxide, flame, and smoke sensors.

5.5.7 System Configuration

The previous sections have described in detail, the individual elements that combine to implement the proposed system architecture. On the combined system, a user can login to monitor and control the HAS's end devices, using one of three user interface devices (ZigBee remote control, Wi-Fi remote control, and Remote access device). All the messages from remote users, using the Internet for communications, are sent to the home's IP address. The received messages are forwarded to the home gateway's IP address on the local Wi-Fi network, through a Wi-Fi enabled ADSL modem. Similarly, messages from the local users, using devices connected to the Wi-Fi network for communications, are forwarded to the home gateway's IP address. Once the home gateway has received the messages, they are forwarded to the virtual home. Messages from the ZigBee controller are sent directly to the end devices, over the ZigBee network. The virtual home checks the security and safety of all received messages. The messages that fail to validate are rejected and the validated messages are forwarded to the destination device on the real home network. All responses from the device (i.e. acknowledgments, device status notifications, sensor readings) are relayed from the device, through the ZigBee network to the virtual home, through the home gateway, across the Wi-Fi network and, where appropriate, across the Internet to remote users.

5.6 Evaluation

The implemented system is evaluated both quantitatively and qualitatively. To demonstrate the feasibility and effectiveness of the proposed system, four devices, a light switch, radiator valve, safety sensor and ZigBee remote control are developed and integrated with the HAS. The system is subjected to a cycle of strenuous operations to simulate a high level of everyday usage. The light state is changed 20 times using the ZigBee remote control and 20 times using the Wi-Fi controller. Similarly, the radiator valve state is changed 20 times using the ZigBee controller and 20 times using the Wi-Fi controller. The experiments show that the devices functioned correctly 100% of the time. Table 5-1 provides a summary of the average delay between request and implementation of the requested change using the Zigbee and Wi-Fi controllers.

Table 5-1: ZigBee and WI-FI controller access delay

	Light Switch	Radiator Valve
ZigBee Controller access delay in ms	670	*N/A
Wi-Fi Controller access delay in ms	1337	613

*N/A indicates that the time delay was too short to be recorded by the test equipment.

As Table 5-1 indicates, the average access delay is greater for the Wi-Fi controller than for the ZigBee controller. The ZigBee controller has an average access delay of 670ms (minimum 429ms, and a maximum of 745ms) while controlling the light switch, whereas the access delay incurred for controlling the radiator valve is small and cannot be measured with the available equipment. This implies that the majority of the access delay for controlling the light switch lies in the actuation of the light switch and subsequent bulb state change and is not attributable to the method of control. This is shown with a N/A in Table 5-1. Taking this into account the access delay for the light bulb (1337 ms) can be adjusted by removing the 670 ms average access delay attributed to the switch actuation to provide a more realistic access time for the Wi-Fi controller of 667ms. The average adjusted access delay for the light switch, using the Wi-Fi controller, is supported by the access delay recorded for the radiator valve of an average 613ms (a minimum of 478ms and a maximum of 678ms).

The viability of the home automation test-bed is evaluated through the real world testing of the proposed system with the developed radiator valve. The radiator valve, as depicted in Figure 5-6 (b), is tested in a real test house. The radiator valve is located in the test house's living room, on the ground floor as depicted in Figure 5-7. The radiators existing thermostatic radiator valve (TRV) is replaced with the prototype automatic radiator valve. The local controller is put on a desk 2m away from the radiator and connected to a laptop. This configuration allows test software running on the local controller to print out the desired temperature set by the user, current temperature around the radiator and time taken to reach the desired temperature by the automatic radiator valve. Figure 5-8 shows the experimental environment.

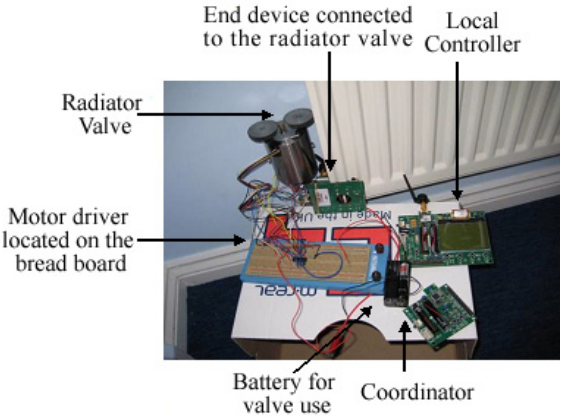

Figure 5-7: Automated radiator valve experiment

Figure 5-8: The experimental environment

The results of the experiments are summarised in Figure 5-9. The graph shows the desired temperature set by the user (Set Point) against the actual temperature (Measured Value) of the radiator at a regular interval of 15 minutes. As depicted, the actual temperature of the radiator quickly adjusts to the desired temperature set by the user, and this holds true for most temperature ranges set by the user. However, the actual temperature cannot reach $25\,^{o}C$, it is surmised that the radiator is too small to heat such a large room to this temperature. The evaluation of the radiator valve shows the applicability of the proposed test-bed with a real world product. The experimentation highlights that a radiator valve can successfully be implemented using the ZigBee communication standard and monitored and controlled using the proposed system. This successful evaluation supports and demonstrates the potential of the proposed system to be easily adaptable from the lab environment to the commercial market. Thus, providing an ideal test-bed for the evaluation of the existing security approaches and those proposed and presented in the following chapters.

For the qualitative analysis of the proposed system, a focus group, held on the 4th of March 2008, is used to evaluate the end user's perspective of the proposed architecture and obtain feedback as to areas for further development of the test-bed. The focus group consisted of ten members from a UK Housing Association (HA) who were chosen to reflect the views of the end customers. From the comments made, the majority of participants feel, that the proposed system's ability to remotely diagnose and check potential errors with systems such as communal lighting provides an attractive feature.

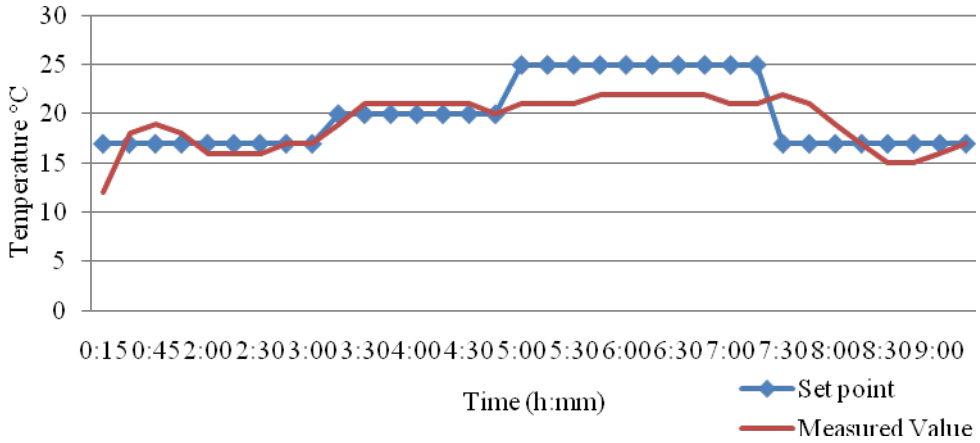

Figure 5-9: Set temperature and measured temperature

Currently the HA spends approximately £100k on monitoring and maintaining communal lighting. The ability to detect when lighting has malfunctioned without physical human monitoring would help the HA make significant savings and incentivise the investment and adoption of such a system. Additionally, the flexible and extensive range of interfaces offered for the control and monitoring of devices connected to the home automation network is felt to be an attractive feature. It is felt that this feature benefits people with mobility problems the most.

5.7 Conclusions

This chapter has identified and discussed five areas that have hindered consumer adoption of home automation technology. Briefly, the areas include the complexity and expense of the architectures adopted by existing systems, the intrusiveness of the system installations, the lack of interoperability between different home automation technologies, poor inconsistent approaches to security and safety, interface inflexibility, and the lack of interoperability between systems

developed by different manufacturers that utilise the same technology. The analysis of the latest home automation research and consideration of the five hindrances have lead to the design and development of a ZigBee-based home automation test-bed. The home automation test-bed was developed as part of a TSB funded home automation project (indeedNET 2007). The ZigBee based HAS's architecture and home gateway, see Figure 5-1, were designed and implemented. The development of the home automation network involved collaboration between colleagues. Moreover, colleagues developed the automated devices, such as the automated light and local controller to test the correct functionality of the home automation network. The extensive evaluation of the developed HAS, including the potential of the HAS as a test-bed for the evaluation of DoS attacks and defences, were conducted. The participation in a TSB funded project allowed for the creation of a fully comprehensive test-bed that otherwise would have been outside the scope of the thesis.

The feasibility and appropriateness of the proposed test-bed architecture and technology has been successfully evaluated both through experimentation and user trials. The ZigBee based local controller and remote control have been shown to successfully send user commands to the respective device and receive acknowledgments of commands in 100% of the experiments conducted. Moreover, the experimentation have highlighted the stability of the architecture adopted, including the minimal impact of the inclusion of the virtual home on the system's performance. The ZigBee access delay while controlling the radiator valve is too small to be recorded with the available equipment. Moreover, the access delay while controlling the radiator valve using the Wi-Fi based controller is on average 613ms (a minimum of 478ms and a maximum of 678ms). The potential for successful coexistence and interoperability of Wi-Fi and ZigBee has been practically proven through the implementation of the technologies as part of the HAS test-bed. Moreover, focus group sessions have shown a positive attitude towards the developed system and significant support for the diverse modes of control, monitoring, and integration with existing home networks such as Wi-Fi. Hence, supporting the viability of the home automation test-bed for evaluating existing security vulnerabilities in the design of WSN based HASs and the proposed security approaches suggested in the following chapters.

Chapter 6

Increasing Third-Party Resistance to DoS Attacks

6.1 Background and Motivation

The literature review (see Chapter 3) has highlighted that the existing approaches for remotely accessing HASs take a very simplistic view. The approaches assume that an Internet connection with a static IP address is available in the HAS's local environment. In the UK, this is not the case, most Internet service providers (ISPs) provide homes with a dynamic IP address, which changes at regular intervals or when the home's Internet connection is disrupted (Bergstrom et al. 2001). Consequently, remote users may not have access to the current IP address associated with their HAS, preventing them from establishing a remote connection. As a result, third-party based approaches have emerged for mediating the connection between remote users and their respective HAS. However, third party based approaches provide a single point of failure. Moreover, third party based approaches neglect the privacy of communications at the third party, allowing communications to be monitored and manipulated by malicious users with access to the third party (Kara 2001).

The objective of this chapter is to present an analysis of existing remote access approaches and the design and implementation of an improved hybrid scheme for providing secure remote access to HASs. The improved approach takes into consideration special characteristics associated with providing remote access for HASs, such as dynamic IP addresses. Moreover, the approach is designed to offer a robust remote access architecture capable of sustaining greater levels of DoS attacks targeted at the third party, whist providing an improved level of service availability for remote users. Additionally, the approach is designed to overcome privacy issues associated with the existing approaches. The proposed scheme is implemented and evaluated on the home automation test-bed introduced in Chapter 5, further illustrating the effectiveness and practicality of the proposed approach. The following section provides a summary of the different types of remote access approaches, as discussed in Chapter 2, and identifies the weaknesses for accessing WSN based HASs using these approaches. The work presented in this chapter is published in (Gill & Yang 2008a) and (Gill & Yang 2008b).

6.2 Analysis of Existing Remote Access Approaches

There are two primary types of remote access approaches, direct access approaches and third party based approaches. The direct access approaches reviewed are designed for high end, resource rich systems and offer varying levels of acceptable protection. However WSN based HASs have special characteristics, arising from their relatively resource limited nature which culminate in these direct access approaches being inappropriate for use. Following is a summary of the characteristics identified from the research.

- *Dynamic IP Address:* Homes in the United Kingdom predominantly have Internet connections with dynamic IP addresses. This is true for both broadband and dial up connections, although the IP address may change less frequently for broadband connections that are always on. As such, it is not possible for a remote user to know their home's current IP address. Hence, remote users cannot make a remote connection to their home using the existing direct access approaches. Moreover, to achieve true end-to-end security each local device requires a static public IP address. With the limitation on the number of addresses available under IPv4 (Internet Protocol Version 4), it may not be

possible to assign each device with a static IP address. Although with the advent of IPv6 (Internet Protocol Version 6) this problem may be addressed in the future, it is still questionable how a mobile client will know the IP address of multiple devices. Additionally, the use of a static IP address opens up the home to additional security vulnerabilities, providing attackers with a fixed point on the Internet to exploit. For example, in the case of DoS attacks the use of a dynamic IP address increases the difficulty for attackers, distributed across large geographic areas, to identify specific homes to attack. Consequently, even if possible, it may not be desirable to adopt a static IP based approach for HASs.

- *Limited Resources:* Direct access approaches are generally aimed at high-end resource rich devices. Consequently, it is unlikely that WSNs have sufficient resources to adopt the comprehensive set of security mechanisms supported by high-end resource rich devices. For example, some of the reviewed direct access approaches use SSL to provide secure communications and authentication services. However, in general resource limited WSNs, such as ZigBee based WSNs, do not inherently support the security mechanisms required by SSL.

- *Technical Ability:* Direct access approaches place the responsibility for establishing and maintaining security on the owners of the system. In terms of homeowners, it is unlikely the average user's technical ability is sufficient to manage such a system. Moreover, it is questionable if the users of the system alone should be relied upon to effectively maintain the security of potentially critical systems.

Third party based approaches help overcome some of the problems identified with direct access approaches. Homes facilitating third party based remote access approaches can have a dynamic IP address, due to the use of an outgoing persistent connection between the HAS and the third party. Moreover, the emphasis on providing security for the system is placed on the third party. This lowers the amount of technical ability required by the homeowners and reduces the impact of resource limitations, associated with WSN based HASs, on the provision of security by distributing security tasks between the HAS and the third party.

However, there are two primary drawbacks of third party based approaches. Firstly, the centralised third party approach provides a fixed entity on the WWW, providing an easy target for attackers seeking to launch DoS attacks. The consequences of a successful attack include the potential for thousands of homeowners to be prevented from remotely accessing their HAS. Moreover, in the case of telehealth systems, where health providers are prevented from remotely accessing and monitoring patient information, fatalities may occur. Consequently, the vulnerability of existing third-party based approaches to DoS attacks poses a significant challenge for researchers. Furthermore, third-party based approaches require the HAS to be connected to the third party at all times, making it available to the remote user when required. This places a large strain on the third party, wastes significant bandwidth, has the potential to cause communications bottlenecks around the trusted third party, and reduces the resources available for the third party to handle DoS attacks.

Secondly, the third party based remote access approaches currently adopted for accessing HASs, identified from the literature, have a serious security gap at the trusted third party. For true end-to-end security, the third party should not be able to view messages in transit between remote users and HASs. However, in the reviewed approaches the messages between remote users and the respective HAS's are decrypted at the third party to authenticate the sender, validate the integrity of messages, and to identify the intended destination of messages for rerouting to the correct HAS. Although the third party may be a trusted entity with measures in place to protect homeowner's privacy, it cannot be guaranteed that these measures are sufficient. This can be illustrated in several cases in the UK where large organisations have had significant breaches in their security procedures and have lost large amounts of personal information. For example, Virgin lost a computer disk with the details of 3000 customers (ICO 2008), the UK child benefits agency lost two hard drives containing personal information including names, addresses, dates of birth, National Insurance numbers and bank details of 25 million people (Poynter 2008), and the UK Ministry of Defence (MOD) lost information on 600 000 potential recruits (Burton 2008). These examples highlight that even the security procedures of large organisations and governments can fail. Furthermore,

even where the procedures are adequate, employees of organisations cannot always be trusted or relied upon to follow these procedures.

Consequently, an improved remote access approach is required that provides a greater degree of robustness to DoS attacks targeted at the third party and reduces the effect of a successful DoS attack on remote users. Moreover, the approach is required to provide remote access in a way that protects the privacy of homeowners. The following sections introduce the design, implementation and evaluation of such an approach.

6.3 Proposed Remote Access Approach

The development of the proposed remote access approach consisted of three stages. Firstly, during stage-one the existing dominant approach for providing remote access to HAS (GHS), introduced in Chapter 2, is modified to create the Remote Home Server One (RHS-1) approach. The RHS-1 approach overcomes the privacy shortfalls discussed earlier. Secondly, during stage-two a novel approach for providing remote access to HASs called the Remote Home Server Two (RHS-2) approach is proposed. The RHS-2 approach provides a lightweight approach for providing secure remote access to HASs. Moreover, the RHS-2 approach drastically reduces the strain placed on the third parties resources. Freeing resources to better withstand DoS attacks. Thirdly, during stage three the RHS-1 and RHS-2 approaches are combined to provide a new and novel hybrid approach robust enough to provide the optimal level of remote services for homeowners, whilst the third party's services are under a sustained DoS attack.

6.3.1 Remote Home Server Approach – Stage One

The RHS-1 approach consists of the remote client, Remote Home Server (third party server) and the home automation test-bed. The RHS-1 approach consists of three phases, the initialisation phase, secure session establishment phase and the communication phase.

6.3.1.1 Initialisation Phase

The RHS-1 approach requires the pre-distribution of two keys. Firstly a server master key (K_M) is distributed to the HAS, RHS and mobile client. Secondly

a client master key (K_C) is distributed to the HAS and mobile client. There are a number of methods for generating and distributing secret keys. A discussion of these methods is outside the scope of this thesis. For the proposed approach, a secure random key generator application is used to generate the master keys. The keys are then manually distributed by the homeowner to the respective entities. The master keys are generated and distributed depending on how often the homeowners wish to change the master keys. The more often the master keys are changed and distributed the more secure the system will remain. However, as with the renewal of keys for existing wireless technologies available in homes, such as Wi-Fi, a relatively infrequent distribution of keys is sufficient for HASs. Consequently, the manual distribution method offers a relatively cheap and efficient method for key distribution. The pseudo code for the secure cryptographic key generation algorithm is depicted in Figure 6-1.

Cryptographic Key and Initialisation Vector Generation Pseudo Code

```
Step 1. Call the function to securely generate a 16 byte AES cryptographic key
        Function GenerateKey ()
        {
Step 2. Generate a secure random value longer than 16 bytes
        SecureRandom sr = new SecureRandom();
Step 3. Initialise the master key and initialisation vector with data from the secure random
        value
        masterKey = new byte[16];
        sr.nextBytes(masterKey);
        initilisationVector = new byte[13];
        sr.nextBytes(initilisationVector);
        }
```

Figure 6-1: The pseudo code for generating the cryptographic keys and initialisation vectors

6.3.1.2 Secure Session Establishment Phase

To increase the security of the system, the previously distributed master keys are used to distribute randomly generated session keys. This reduces the amount of cipher text sent across the Internet encrypted with the master keys, which can be analysed to derive the master keys. Consequently, the master keys need to be changed less frequently. The general procedure for securely distributing two session

keys between two participants, participant A acting as the client and participant B acting as the server, is as follows:

Participant A generates a random number called a Nonce and encrypts it with K_M. The encrypted message is sent to Participant B. Participant B decrypts the incoming message and increments the extracted Nonce and randomly generates a session key (K_{SA}). Both the Nonce and session key are encrypted with the previously distributed K_M and sent to participant A. Participant A decrypts the incoming message and increments the Nonce and encrypts it with the received session key K_{SA}, before returning the message to participant B. Once participant B has successfully decrypted the message and established that the nonce has been successfully incremented, session keys have been successfully exchanged and a secure session between participant A and B has been established. All future communications between participant A and B will be encrypted with K_{SA}, providing message confidentiality. Only entities with the K_M can communicate with each other, helping authenticate participants. Moreover, the use of the Nonce when

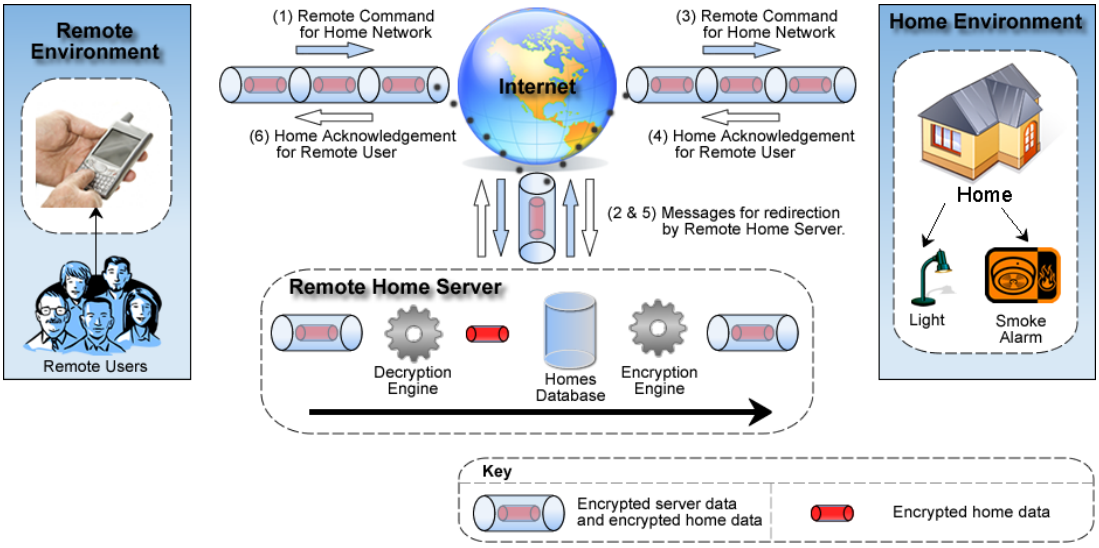

Figure 6-2: Remote home server conceptual diagram

combined with a unique session key helps stop a potential attacker from masquerading as the trusted third party or remote user and replaying messages. Each session key is used for "SKx" number of messages, where "SKx" is a previously defined number of messages. The system administrator must choose "SKx" by weighing up the decrease in performance due to renegotiating a session

key with the potential risk an attacker may be able to decipher a session key, if too much cipher text becomes available.

In the RHS-1 approach, the HAS (A) uses the previously described method for creating a secure communications session with the RHS (C) ($K_{SA,}$ N_A) these are encrypted to make message A (M_A). When a mobile user (B) wishes to communicate with the HAS, it similarly establishes a secure session with the RHS (K_{SB}, N_B) these are encrypted to make message B (M_B).

The mobile user creates a direct secure session with the HAS, by tunnelling messages through the RHS, see Figure 6-2. As described in the method for securely establishing sessions, the mobile client generates a random session key (K_{SC}) and a random nonce (N_C), which are encrypted with the previously distributed K_C (It should be noted that only the mobile client and HAS possess this key) to form a new message M_C. The message M_C is combined with $N_{B,}$ properly incremented, and information required by the RHS to successfully redirect the message to the HAS, such as a Home ID. This is further encrypted with K_{SB} to form M_B and sent to the RHS.

The RHS decrypts M_B and obtains M_C, N_B and the Home ID. The RHS looks up the associated connection with this Home ID in the Homes database. The M_C is then combined with the appropriate N_A and encrypted with $K_{SA,}$ to form M_A, and sent to the HAS. It should be noted that at no time has the RHS been able to see the plaintext message between the mobile client and HAS (M_C) containing K_{SC}. The HAS first decrypts M_A using K_{SA} to obtain M_C and $N_{A.}$ Once the N_A has been verified, M_C is decrypted using K_C to obtain K_{SC}. At this stage both the mobile client and the HAS have K_{SC}, the HAS increments N_C and returns it encrypted with K_{SC}, as before through the established secure sessions, through the RHS to the remote client for verification that the HAS is in possession of the session key (K_{SC}) and ready to begin the communications phase.

6.3.1.3 Communication Phase

Once the mobile client and HAS have exchanged a session key this is used to encrypt messages, and tunnel them through the existing secure sessions between the mobile client and RHS and the RHS and HAS, as shown in Figure 6-2.

The secure distribution of sessions keys through the pre-existing secure sessions between the client and HAS overcomes the previously identified security gap at the third party. In essence a secure tunnel between the client and HAS has been established through the pre-existing secure tunnels between the client and RHS, and the HAS and the RHS. Unlike the existing approaches, at no point in the communication stage is the RHS aware of the session key used to encrypt personal information or the information necessary to derive the session key, providing an increased level of privacy for homeowners.

6.3.2 Remote Home Server Approach – Stage Two

The RHS-2 approach consists of a remote user, RHS and HAS. The RHS-2 approach consists of five phases, the initialisation phase, secure session establishment phase, IP address update phase, IP address check phase and the communication phase.

6.3.2.1 Initialisation Phase

The RHS-2 approach requires the pre-distribution of two keys. Firstly, a server master key (K_M) is distributed to the HAS, RHS and mobile client. Secondly,

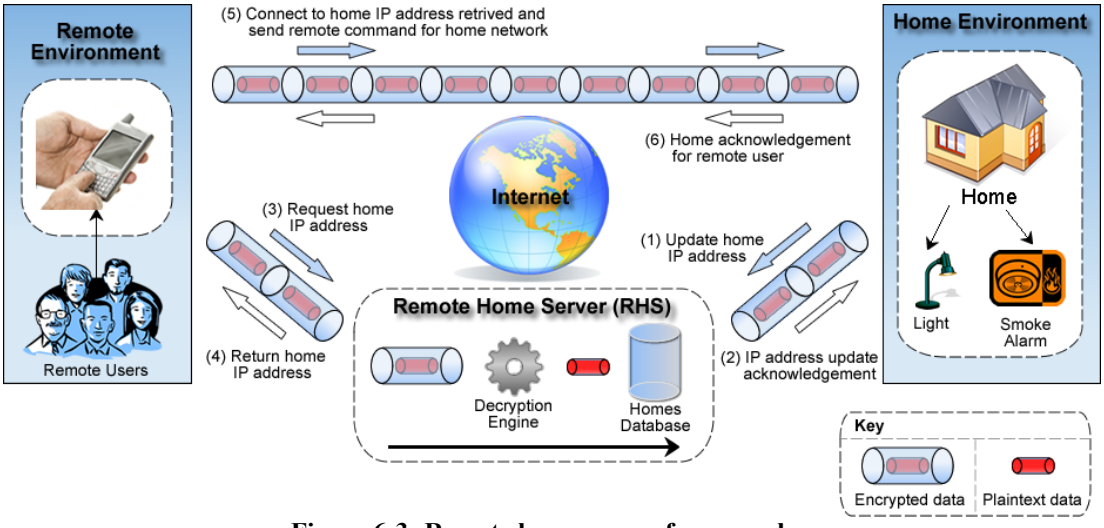

Figure 6-3: Remote home server framework

a client master key (K_C) is distributed to the HAS and the mobile client. The master keys are generated and distributed in the same manner as for the previous approach.

6.3.2.2 Secure Session Establishment Phase

The secure session establishment phase for the RHS-2 approach is the same for the RHS-1 approach (see Section 6.3.1.2). For the RHS-2 approach the "secure session establishment phase" is implemented during the "*IP Address Update Phase*", "*IP Address Check Phase*", and the "*Communications Phase*".

6.3.2.3 IP Address Update Phase

The HAS establishes a secure session using the previously described method with the RHS, using the previously distributed K_M. The homes current public IP address is then sent to the RHS for storage in the RHS homes database. The RHS identifies which homes IP address field in the homes database should be updated by contrasting the login details of the connection with those stored in the homes database. The update period for the home database is "IPx" seconds, this period is chosen to minimize the amount of bandwidth used while minimizing the time where the homes IP address may be out of date, and preventing a remote user from connecting. Once the IP address has been successfully updated by the RHS, an acknowledgment is sent to the HAS. This allows any failures in the RHS to be detected. This is depicted as stage (1) and (2) in Figure 6-3.

6.3.2.4 IP Address Check Phase

The remote user establishes the IP address of the HAS through two stages. Firstly, the remote user checks to see if a stored IP address, from a previous connection is still valid. This is done by attempting to successfully establish a secure connection with the HAS at the previously stored IP address. If the device at this IP address is not capable of successfully decrypting the message, correctly incrementing the nonce and re-encrypting the data the previously stored IP address is considered invalid. In most cases in the UK where a broadband connection is available, the IP address will change infrequently and as such in most cases a previously stored address will be valid. Secondly, if the previously stored IP address is found not to be valid the remote user will establish a secure connection with the RHS, as previously described, using K_M. The remote user then requests the IP address of the home associated with the login credentials used for the current connection, from the RHS. The corresponding IP address is returned to the remote client from the RHS. At this point, the remote user has a high probability of

possessing the correct IP address. However, if the connection cannot be successfully established, or the connection is lost the RHS is re-queried until the correct IP address is obtained. This is depicted in stages (3) and (4) in Figure 6-3.

6.3.2.5 Communication Phase

Once the remote client has successfully obtained the correct IP address, a secure connection is established directly with the HAS, as previously discussed. However, K_C is used as the master key, hence only the remote client and HAS are capable of establishing secure communications because no other parties share K_C. Once a secure connection has been established the remote client sends the desired commands to the HAS and correspondingly the HAS responds by sending the appropriate acknowledgements and data to the remote client. This is depicted in stages (5) and (6) in Figure 6-3. If at any point the connection is lost, the "IP Address Check Phase is re-entered" in an attempt to re-establish communications. This approach significantly reduces the strain placed on the RHS, compared to the RHS-1 approach and the popular remote access approaches for HASs, which require all of the supported HASs to maintain a permanent connection with the third party. In the RHS-2 approach, the remote users are only required to connect to the RHS when the HASs IP address has changed, since the previous access. This allows the RHS to provide services for significantly more HASs and frees up resources to deal more effectively with DoS attacks. Additionally, during an effective DoS attack against the RHS, all of the remote clients that have previously connected to their HAS, whose homes IP address has not changed since the last connection, remain unaffected by the DoS attack until the IP address of the respective HAS changes.

6.3.3 Hybrid Remote Access Approach – Stage Three

During the third stage, the previously introduced RHS-1 and RHS-2 communications approaches were integrated to produce a hybrid communications approach. The RHS-1 and RHS-2 approaches operate separately as described in the previous stages. However, a switching mechanism is introduced at the mobile client interface, see Figure 6-4, 6-5, and 6-6, at the home server, see Figure 6-7, and 6-8 for switching from third party mediated communications using the RHS-1 communications approach, which offers the greatest security to the RHS-2

communications approach, during periods where the RHS is not available due to DoS attacks.

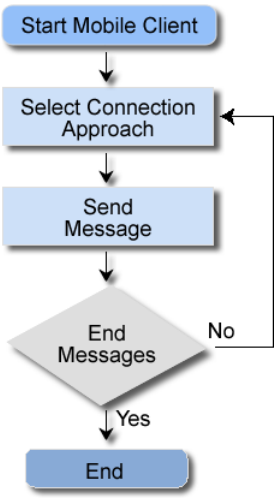

Figure 6-4: High level mobile client communications flow chart

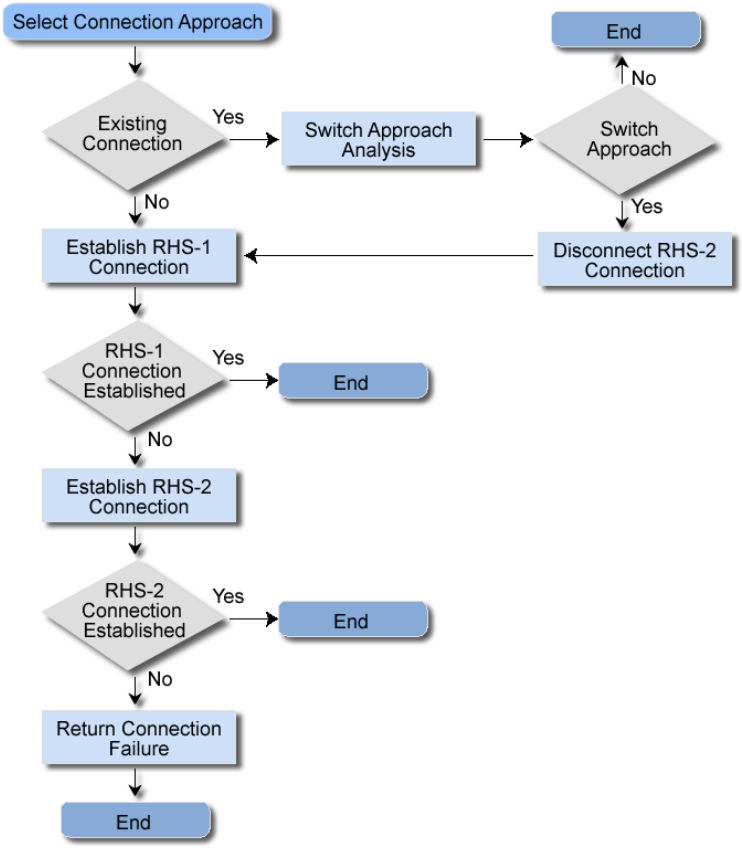

Figure 6-5: Low-level mobile client and home server connection approach selection flow chart

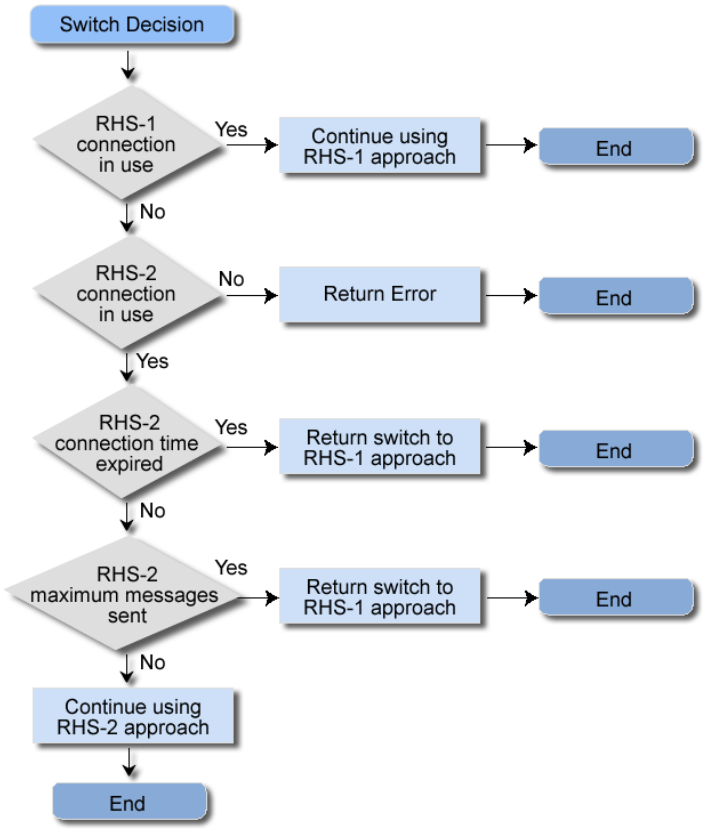

Figure 6-6: Low-level mobile client connection approach switching decision flow chart

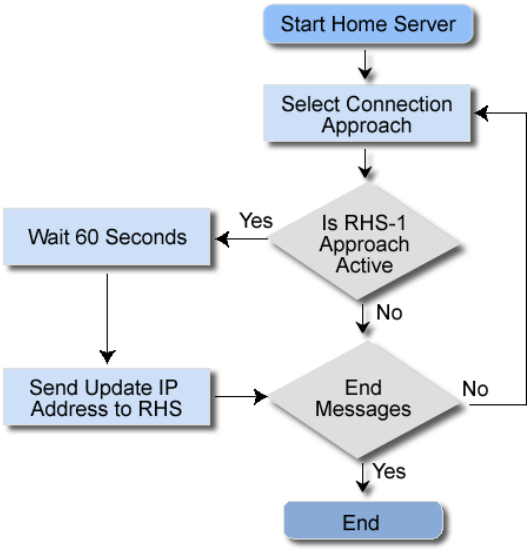

Figure 6-7: High level home server communications flow chart

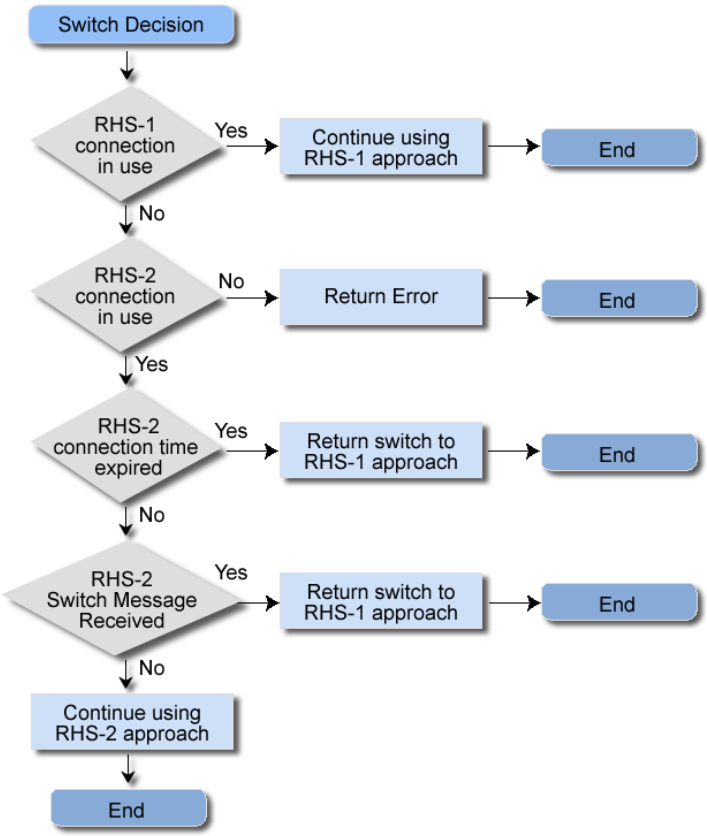

Figure 6-8: Low-level home server connection approach switching decision flow chart

The switching mechanism at the mobile client starts with the mobile client creating a connection to the HAS, using the RHS-1 communication approach to create a mediated connection. After each message is sent to the HAS through the RHS a check is conducted to ensure the connection has not been dropped. If the connection has not been dropped, communications continue until the communication session has ended. If the connection is dropped, the mobile client attempts to re-establish communications for a user-defined period of time (t_{mc1}). If the connection cannot be successfully re-established, the switching mechanism changes the communications approach from the RHS-1 to the RHS-2 communications approach, for N messages or until a user-defined period of time (t_{mc2}) expires. For t_{mc2} the mobile client continues to communicate using the RHS-2 communications approach. After this period has expired, the switching mechanism returns to using the RHS-1 communications approach to check if communications can be re-established with the RHS. If the switch is successfully made, the mobile client switches back to the RHS-2 communications approach, sends a message to the Home Server to change approaches, and then returns to using the RHS-1

communications approach. This checking and switching procedure is repeated until the end of communications.

For the mobile client to form a successful connection with the HAS, the home server must be in RHS-2 communications mode before the onset of communications. Figure 6-7 and 6-8 illustrates the switching mechanism used by the home server. The switching mechanism adopted at the home server is similar to that adopted by the mobile client. Initially the home server establishes a connection with the RHS. At regular intervals (t_{hs1}), amongst normal mediated communications, the home server sends the homes current IP address to the server for storage. After each IP address update cycle, a check is conducted to ensure the connection has not been dropped. If the connection has not been dropped, communications continue until the communication session has ended. If the connection has been dropped, the mobile client attempts to re-establish communications for a user-defined period of time (t_{hs2}). If the connection cannot be successfully re-established, the switching mechanism changes the communications approach from the RHS-1 to the RHS-2 communications approach. The home server remains in the RHS-2 communication mode until the mobile client sends the home server a message to switch back to the RHS-1 communication approach or until a user defined timeout (t_{hs3}) is triggered after a period of inactivity.

The next section introduces the implementation of the proposed RHS-1 and RHS-2 hybrid communications approach. Followed by the analysis of the strengths and weaknesses of the proposed and existing access approaches, and the evaluation of the proposed hybrid remote access approach as a means to overcome these weaknesses and provide a remote access approach more resilient to DoS attacks.

6.4 Remote Access Approach Implementation

As depicted in Figure 6-9 the hybrid RHS-1 and RHS-2 approach consists of five components. There is the RHS client that resides on the remote user's mobile device. There is the RHS and RHS Database Sever that reside on the high-end servers of a trusted third party. Finally, there is the Local Home Client and Local Home Server that reside on a home gateway, discussed later, that forms the connection between the RHS and the home automation test-bed, which resides in

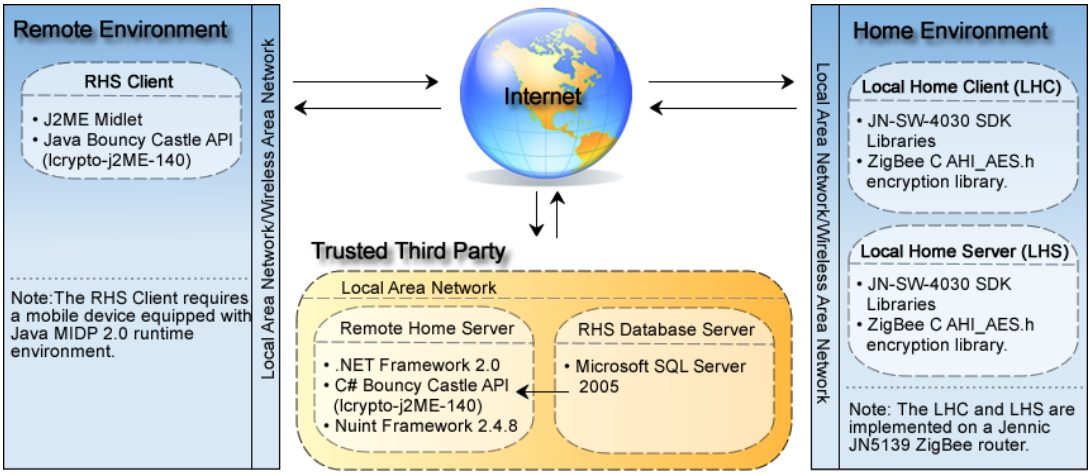

Figure 6-9: Remote home server system architecture

the home environment. This section reviews the detailed hardware and software implementation of the conceptual design of the hybrid RHS-1 and RHS-2 approach described in the previous section. For more information regarding the design and implementation of the home automation test-bed, please refer to Chapter 5.

6.4.1 RHS Client

The RHS client is implemented on a standard mobile phone as a J2ME MIDlet, as depicted in Figure 6-10. The MIDlet is used to provide the TCP connectivity with the RHS during RHS-1 communications and with the RHS and HAS during RHS-2 communications. Moreover, the MIDlet provides the remote user interface for the HAS. The security functions are implemented by integrating the free source Bouncy Castle API with the MIDlet. The use of the Bouncy Castle (Bouncycastle 2009) API allows for the use of a well-established and tested security API. In addition, the previously discussed mobile client switching mechanism is implemented as part of the Java MIDlet. The pseudo code for the mobile client is depicted in Figure 6-11 (a) and (b).

Figure 6-10 RHS client interface on mobile phone

6.4.2 Remote Home Server

The RHS is implemented on a standard laptop. The RHS is coded in C# using the .NET Framework 2.0. Although the .NET Framework provides its own security libraries, resource limitations posed by the home automation test-bed, as discussed later, mean that the .NET framework libraries do not provide the encryption algorithms required. As a result, the C # implementation of the Bouncy Castle API is used to provide the required security functionality. A crucial component of the RHS is the RHS database server. The database maintains information on all the connected homes. The database is implemented using Microsoft SQL server 2005. The RHS mediates communications between the remote client and HAS during RHS-1 communications and provides the remote client with an IP look up service during RHS-2 communications.

Mobile Client Switching Pseudo Code

```
Class Mobile Client{

        long timerStart;
        long  RHS-2 connection time limit = 60000;
        int messageCounter = 0;

        Function startRHS(){

                while (user input) {
```

Step 1: Select and establish a connection approach (RHS-1 or RHS-2) with the WSN based HAS. Repat this step for the duration of the communication.

```
                        string status = "";
                        status = startConnection();
                        Send (Messages);

                        if(Continue using RHS-2 Approach){
                                messageCounter++;
                        }

                        if(status = Connection cannot be established){
                                alert(status);
                                break;
                        }
                }
        }
```

Figure 6-11: (a) Mobile client pseudo code

Mobile Client Switching Pseudo Code

```
        Function startConnection(){

Step 2: Check if there is an existing connection, or if a new connection is needed.

                if(Existing Connection){
                        String decision = "";
                        decision = switchDecision();

                        if(decision == Switch to RHS-1){
                                disconnect.RHS-2 approach;}
                        if(decision == Continue using RHS-1 Approach){
                                return(decision);}
                        if(decision == Continue using RHS-2 Approach){
                                return(decision);}
                        if(decision == Connection cannot be established){
                                return(decision);}
                }

                Open connection RHS-1 (IP Address, Port);

                if(RHS-1 Connection Established){
                        return(RHS-1 communication approach started);
                }else if(RHS-1 communication approach failed){
                        Open connection RHS-2 (IP Address, Port);
                        messageCounter = 0;
                        timerStart = System.currentTimeMillis();}
                if(RHS-2 Connection Established){
                        return(RHS-2 communication approach started);
                }else if(RHS-2 communication approach failed){
                        return(Connection cannot be established);}
        }

        Function switchDecision(){

Step 3: If an existing connection is present check to see of it is a RHS-2 connection and if it
needs to be switched back to a RHS-1 connection to see if the flooding DoS attack against the
RHS has stopped.

                if(RHS-1 Connection Approach in Use){
                        return(Continue using RHS-1 Approach);
                }

                if(RHS-2 Connection Approach in Use){

                        if(timerStart  > RHS-2 Connection time limit){
                                return(Switch to RHS-1);
                        }else if(messageCounter > RHS-2 maximum message limit){
                                return(Switch to RHS-1);
                        }else{
                                return(Continue using RHS-2 Approach);
                        }
                }else{
                        return(Connection cannot be established);
                }
        }
}
```

Figure 6-11: (b) Mobile client pseudo code

6.4.3 Home Gateway

The home gateway (See Figure 6-12) connects the HAS with the Internet. The home gateway forms part of the home automation test-bed described in detail in Chapter 5. In brief, the home gateway provides a mains powered, low cost, and standalone bridge between the Internet and the local home automation network. The low cost nature of the home gateway and the integration of the home gateway with the ZigBee based home automation network provides a good opportunity to test the existing, RHS-1, RHS-2 and hybrid approaches with a real resource limited WSN based HAS. The resource limitations of the home gateway are listed in Table 6-1.

Figure 6-12: Home gateway

The home gateway hosts a local home client and home server. The home client and server applications are implemented on a single ZigBee micro-controller. The micro-controller uses the ZigBee AHI_AES.h library to provide the required

Table 6-1: Home gateway resource limitations

Constraint	Description
Memory	192 KB ROM 96 KB RAM
Processing power	32-bit RISC processor, capable of 16 MIPS
Supported encryption algorithms and modes of operation.	AES ECB AES CCM* AES IEEE CTR

security functionality. Due to the resource limitations, listed in Table 6-1, the choice of encryption algorithms and mode of operation are limited. From the available selection, the AES encryption algorithm is chosen, operating in CCM mode. CCM is a block cipher mode and as such provides both message confidentiality and integrity. Due to memory constraints, it is not possible to implement a separate encryption and integrity-checking algorithm. Moreover, AES CCM is supported by

the Bouncy Castle API for J2ME and C# used on the mobile client and RHS respectively. The local home client is responsible for establishing the secure connection with the RHS and updating the homes IP address stored on the RHS homes database during RHS-2 communications. During RHS-1 communications, the home client is responsible for establishing an outgoing connection to the RHS. The local home server is responsible for accepting and dealing with requests from authorised remote clients for the creation of secure two way communications during RHS-2 communications. The pseudo code for the home gateway is depicted in Figure 6-13.

6.5 Remote Access Approach Evaluation

The evaluation of the remote access approaches consists of three stages. Firstly, a quantitative analysis of the performance of the existing and proposed remote access approaches, including the direct, GHS, RHS-1, and RHS-2 communications approaches, are presented. Secondly, to evaluate the remote access approaches from a different perspective, the findings from a qualitative study examining the strengths and weaknesses of the different approaches are presented. Thirdly, the potential of the proposed hybrid approach, designed to overcome some of the identified weaknesses, for providing increased resistance to DoS attacks is evaluated.

Home Server Switching Pseudo Code

```
Class Home Server{
        long timerStart = System.currentTimeMillis();
        long  RHS-2 connection time limit = 300000;
        Function startRHS(){

                while (End Message Received = false) {

Step 1: Select and establish a connection approach (RHS-1 or RHS-2) with the WSN based HAS.
Repat this step for the duration of the communication.

                 string status = "";
                 status = startConnection();
                Redirect(Redirect messages received from RHS to WSN based HAS);
                if(RHS-1 communication approach started  or Continue using RHS-1 Approach){
                                if(Timer != Active or Expired){
                                        Timer(60000ms, SendIP address); }
                        }
```

Figure 6-13: (a) Home server pseudo code

Home Server Switching Pseudo Code

```
                    if(status = Connection cannot be established){
                        alert(status);
                        break;}
                }
}

Function startConnection(){
```

Step 2: Check if there is an existing connection, or if a new connection is needed.

```
                if(Existing Connection){
                    String decision = "";
                    decision = switchDecision();

                    if(decision == Switch to RHS-1){
                        disconnect.RHS-2 approach;}
                    if(decision == Continue using RHS-1 Approach){
                        return(decision);}
                    if(decision == Continue using RHS-2 Approach){
                        return(decision);}
                    if(decision == Connection cannot be established){
                        return(decision);}
                }

                Open connection RHS-1 (IP Address, Port);
                if(RHS-1 Connection Established){
                    return(RHS-1 communication approach started);
                }else if(RHS-1 communication approach failed){
                    Open connection RHS-2 (IP Address, Port);
                    timerStart = System.currentTimeMillis();}
                if(RHS-2 Connection Established){
                    return(RHS-2 communication approach started);
                }else if(RHS-2 communication approach failed){
                    return(Connection cannot be established);}
}

Function switchDecision(){
```

Step 3: If an existing connection is present check to see of it is a RHS-2 connection and if a switch message has been received or RHS-2 timeout has occurred then switch to RHS-1 to see if the flooding DoS attack against the RHS has stopped.

```
                if(RHS-1 Connection Approach in Use){
                    return(Continue using RHS-1 Approach);}
                if(RHS-2 Connection Approach in Use){
                    if(timerStart  > RHS-2 Connection time limit){
                        return(Switch to RHS-1);
                    }else if(messageCounter > Switch Message Received){
                        return(Switch to RHS-1);
                    }else{
                        return(Continue using RHS-2 Approach);}
                }else{
                    return(Connection cannot be established);}}}
```

Figure 6-13: (b) Home server pseudo code

6.5.1 Performance Analysis of Remote Access Approaches

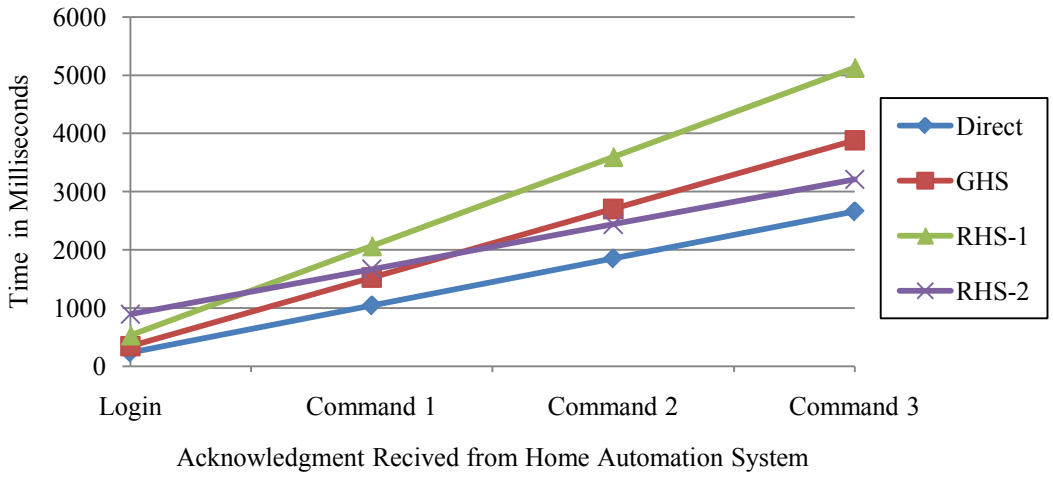

Figure 6-14: Comparative analysis of time delay associated with different remote access approaches

For the performance analysis of the remote access approaches, the existing direct access and GHS approaches are implemented alongside the proposed RHS-1 and RHS-2 approaches and integrated with the home automation test-bed. The approaches are used to control devices on the home automation test-bed. The time taken for a user to login, establish secure communications, and subsequently send and receive acknowledgments for three consecutive commands is recorded. This exercise is further repeated 10 times. The average results of these experiments are depicted in Figure 6-14. As can be seen, the direct access approach is the fastest of the four approaches analysed to login, share secure parameters and send three consecutive commands in all of the 10 trials, taking on average 2661ms (a minimum of 2604ms and a maximum of 2793ms). The proposed RHS-2 approach provides the second fastest performance in all of the 10 trials, a minimum of 19,8% (3189ms) slower, on average 20.59% (3209ms) slower, and a maximum of 20.80% (3215ms) slower. The GHS approach is the third slowest in all of the trials, being a minimum of 39.23% (3705ms) slower, on average 45.81% (3880ms) slower, and a maximum of 46.60% (3901ms) slower. The RHS-1 approach is by far the slowest in all of the 10 trials, being a minimum of 86.85% (4972ms) slower, on average 92.78% (5130ms) slower, and a maximum of 95.60% (5205ms) slower. From this analysis, and based solely on performance, the direct access approach seems to offer the best performance. However, due to the characteristics of HASs, where the homes IP

address is dynamic and subsequently cannot be known in advance by remote users, the direct access approach is not viable for HAS. Moreover, the RHS-2 approach is only on average 20.59% slower than the direct access approach on the first login, after a home's IP address has changed. On subsequent accesses, the RHS approach uses a previously stored IP address and offers the same performance as the direct access approach. Subsequently, it can be surmised that the RHS-2 approach offers a good level of performance, whilst also providing an improved level of communication privacy for homeowners. Additionally from the performance analysis, the GHS and RHS-2 approaches seem to offer a relatively poor performance. However, this is only a relative conclusion. In reality, the performance of all the remote access approaches may offer an acceptable level of performance for users. The acceptability of the different performance offered by different access approaches to users is investigated further in Chapter 8.

6.5.2 Qualitative Analysis of Remote Access Approaches

Following is a qualitative analysis, where the strengths and weaknesses of the access approaches are contrasted in order to evaluate the approaches from a different perspective and add to the conclusions from the previous quantitative analysis. The strengths of the approaches are conversely the weaknesses of other approaches. Consequently, the strengths and weaknesses are categorised as those, which during the study were expressed in a positive way (Strengths) and those, which were expressed in a negative way (weaknesses).

6.5.2.1 Strengths of Different Remote Access Approaches

- ***Improved Service Availability***: The RHS-2 approach stores the IP address of previous connections. Due to the nature of broadband connections in the UK the IP address of most connections will change infrequently. Subsequently, if the RHS is successfully targeted by a DoS attack, and blocked from providing remote services to legitimate clients, there is still a significant possibility that a successful connection can be established using the RHS-2 approach. Whereas, both the GHS and RHS-1 approaches will not function.

- ***Distribution of Internet Traffic***: The RHS-2 approach does not channel all traffic through a trusted third party. Consequently, the risks of communication

bottle necks around a trusted third party, such as the RHS, arising from floods of legitimate traffic or DoS attacks is reduced.

- ***End-to-End Security***: In both the RHS-1 and RHS-2 approach, only the remote client and HAS share the secret key used to encrypt sensitive data. As such, only the remote client and HAS can decipher messages. Unlike existing approaches, such as the GHS approach, the third party is not able to decipher communications between the remote client and home server. Moreover, while the Home Server's IP address does not change the RHS in the RHS-2 approach does not know when and how long remote users connect to their respective home server. Thus providing end-to-end security and increasing the user's privacy.

- ***Reduced Ciphertext Availability***: In the RHS-2 approach, the RHS provides users with the home's IP address. After which the communications between the remote user and HAS are direct. Hence, the amount of ciphertext available at the RHS for any attacker to decipher is vastly decreased.

- ***Reduced Connection Time***: The initial connection with the HAS is slightly longer using the RHS-2 approach than the direct access approach, see Figure 6-14. However, subsequent connections are direct until the homes IP address changes, the average connection speed is significantly reduced compared to other third party based approaches such as the GHS and RHS-1 approaches.

6.5.2.2 Weaknesses of Different Remote Access Approaches

- ***Modem Configuration***: Systems adopting the direct access or RHS-2 approaches require any modem based firewall to be configured to allow TCP/IP connections on a certain port. Moreover, NAT must be configured to redirect traffic on this port to the home server, which must be located at a fixed local private IP address. Although, this configuration is only required once during the system's installation, the third party based approaches (RHS-1 and GHS) do not require any such configuration due to the nature of most firewalls and NATs, which generally do not apply rules to outgoing connections.

- ***Traffic Analysis***: In the direct and RHS-2 approaches, communications are not routed through a third party, they are direct with the HAS. This can allow an attacker to detect which HAS is linked with a particular user and when a user is remotely communicating.

- ***Initial Connection Phase Delay***: During the initial connection, the remote user will try connecting to the HAS using a previously used IP address. If this is found to have changed, the system will then perform an IP address lookup. This adds an access delay for the connection compared to other approaches. However, the IP address of broadband connections changes infrequently, therefore the decrease in the average connection times compared to existing approaches is unlikely to have a significant impact on the remote access performance.

- ***Home Server Security Resource Constraints***: The home server is considerably more resource constrained than the RHS. As a result, the security mechanisms employed on the home server do not provide the same level of security as those employed on the RHS. Consequently, the lightweight RHS-2 access approach and other direct access approaches are not suitable for home automation applications where security is of greater importance than the speed of operations. In such situations, the third party based approaches (RHS-1 and GHS) offer remote access approaches that provide more advanced security mechanisms.

- ***Home Server Security Expertise Constraints:*** In the direct access and RHS-2 approaches, the third party (RHS) either plays no role or provides simple services not related to the security of communications. The responsibility for maintaining the security of the home gateway and consequently the remote access approach is that of the system's owner. In the case of homeowners, it is unlikely they have the knowledge to maintain the security of such systems. The third party based schemes such as GHS and RHS-1 approach place a greater percentage of the responsibility for maintaining security on security experts at the third party. Consequently, for critical applications or the protection of homeowner privacy the RHS-1 and GHS approaches offer far greater security.

- ***Content Modification Services:*** There are numerous applications where a homeowner may actively wish a service provider to have access to certain communications. For example, a homeowner may wish to provide access to communications relating to the homes energy usage to third parties that may process the data, contrast it with other collected data, and return information that is more meaningful to the remote users. However, such content modification services are only possible using third party mediated communications such as the GHS and RHS-1 communications approaches. Moreover, the dual encryption nature of the RHS-1 approach allows information to be made selectively available to a third party, unlike the GHS approach.

The qualitative analysis shows that although the performance analysis indicates that the RHS-2 is the optimal approach, from a qualitative perspective the third party based approaches ranked at the bottom of the performance analysis, offer other benefits such as added security and provision of content modification services. It can be concluded that the proposed hybrid communications approach provides a more comprehensive solution than the approaches alone. Thus, during a critical session, such as controlling a telehealth or security system, where communications security and anti-traffic analysis measures are of greater importance than the speed of communications, the RHS-1 approach offers the most effective option. Moreover, in systems where content modification services are required from a third party, the RHS-1 approach offers the only solution. Conversely, during non-critical operations, such as controlling a home's lighting, or where the RHS server is not available due to a DoS attack the RHS-2 approach, which offers less security however a 48.13% performance increase in the speed of operations, provides the most efficient and effective communications approach.

6.5.3 Analysis of the Hybrid Remote Access Approach

The analysis of the hybrid remote access approach consists of two stages. Firstly, the performance of the different remote access approaches during a scenario involving a DoS attack targeted at the third party is contrasted. Secondly, for the same scenario the performance of the hybrid remote access approach for dealing with the DoS attack is contrasted.

Firstly, for the comparison of the performance of different approaches while under a DoS attack a scenario is presented, where health professionals remotely control a telehealth system. The home automation test-bed plays the part of the telehealth system. The remote users use the direct access approach for monitoring and controlling the telehealth system. During operations, an unknown attacker performs a flooding DoS attack on the RHS, which prevents remote users from accessing the RHS server. The attacker ends the attack after a duration of 5000ms. The experiment is then repeated 10 times for each of the communications approaches, including the GHS, RHS-1 and RHS-2 approaches in place of the direct access approach. Figure 6-15 shows the averaged results of the 10 trials, for each communication approach.

As the qualitative analysis predicts, the third party based remote access approaches (GHS and RHS-1) fail to provide remote access for the duration of the DoS attack during which the RHS is inaccessible, in the case of all of the 10 trials. However assuming the home's IP address is known, using the direct access and RHS-2 approaches the remote users effectively communicate with the telehealth system, in all of the 10 trials. As previously discussed, the direct access approach is not practical for HASs, where the IP address of the home is generally dynamic and as such unknown. Consequently, it can be concluded that the RHS-2 approach provides a satisfactory communication approach for non-critical communications, whilst remaining unaffected by DoS attacks targeted at the third party as long as the homes IP address has not changed since a prior communication.

Secondly, the same scenario is repeated with the hybrid approach in place. The hybrid approach adopts the securer RHS-1 approach at the start of communications. An attacker launches an effective DoS attack against the RHS. Once communications are lost between the remote user and RHS the hybrid approach adopts the RHS-2 communications approach. Once the DoS attack has ended and the remote user is able to communicate with the RHS, the hybrid approach switches back to the RHS-1 communication approach. During non-critical communications, the hybrid approach operates in RHS-2 mode. Figure 6-15 shows the averaged effectiveness of the hybrid remote access approach during the discussed attack scenario, from the 10 trials.

During the experiment, the hybrid approach functioned as expected. Communications were interrupted, in all of the 10 trials, however the hybrid approach automatically adjusted from the RHS-1 approach to the RHS-2 approach in all of the 10 trials, taking a minimum of 1648ms, an average of 1770 milliseconds, and a maximum of 1890ms. In the experiments, the hybrid approach retries to connect to the RHS, once the connection is lost. Connection attempts are made in the 10 trials for the average time taken to send a command and receive the response from the RHS (1533 milliseconds in the experiments). To decrease the response time required to react to an attack the time-period a service interruption is analysed may be decreased. Alternatively, to increase the accuracy of DoS or service failure detection the time-period an attack is analysed may be increased.

Once the hybrid approach has detected the DoS attack, the hybrid approach remains in the RHS-2 communication's mode for 5 communication attempts or if no communications attempts are made until the predefined timeout (60000ms) expires. Subsequently, the hybrid approach attempts to detect if the DoS attack against the RHS has ended by attempting to reconnect to the RHS using the RHS-1 approach. If the attack has not ended the hybrid approach remains in the RHS-2 mode for a further 5 communication attempts then repeats the previous steps. The duration the hybrid approach remains in RHS-2 mode and the frequency with which the status of the DoS attack against the RHS is checked, depends on the respective system administrator. A low check rate means the hybrid approach remains in the less secure RHS-2 mode for longer, even when the attack has ended. On the contrary, a high check rate wastes significant resources and adds an average delay of 1770 milliseconds in the experiments to each check phase (The delay consists of login attempt duration (1533ms), RHS-2 login (237ms)).

In the first 23 seconds of the scenario using the hybrid approach 14 commands were sent and acknowledged by the telehealth system, for all 10 of the trials. Whereas, in the first 23 seconds of the scenario using the RHS-1 and GHS approaches 10 and 13 commands were received and acknowledged, approximately 28.6% and 7.14% less than the hybrid approach, for all of the 10 trials. Moreover, the HAS services were unavailable to the remote users, during the attack, whilst using the hybrid approach for a minimum of 2947ms, an average of 3069ms, and a

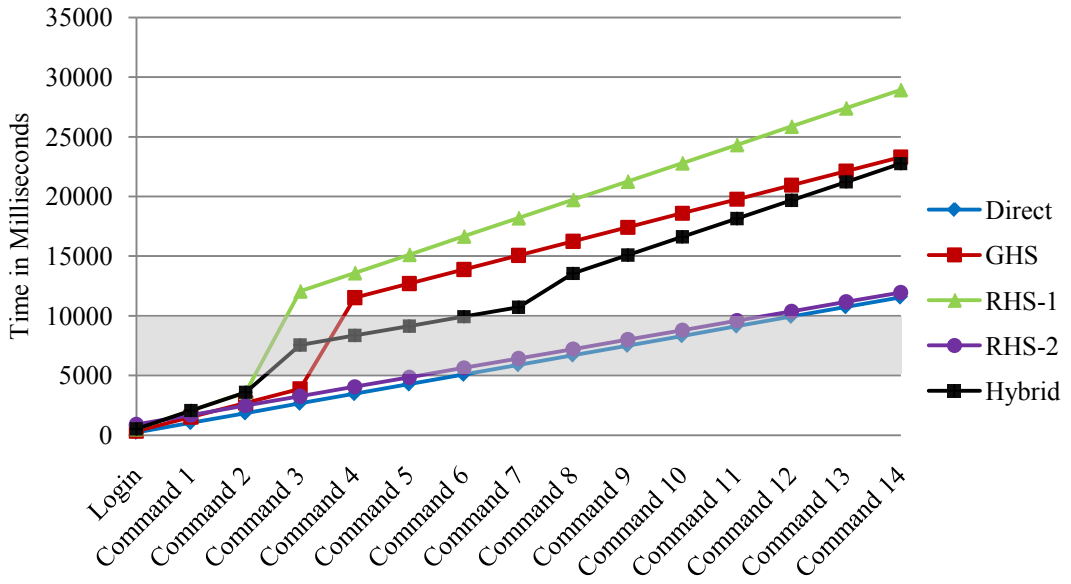

Figure 6-15: Comparative analysis of average time delay of different remote access approaches whilst the RHS is subjected to a DoS attack

maximum of 3189ms, for the 10 trials. During the same duration of attack using the RHS-1 and GHS approaches, the HAS services were unavailable for the 10 trials, an average of 8467ms (a minimum of 8117ms and a maximum of 8668ms) and an average of 7644ms (a minimum of 7549ms and a maximum of 7776ms) respectively. The experiments show over a relatively short duration of time and for a relatively short DoS attack the proposed hybrid approach decreases the time the HAS services were unavailable compared to the RHS-1 approach, in all of the 10 trials by a minimum of 62.34%, on average 63.75%, and a maximum of 65.19%. Moreover, compared to the GHS approach the proposed hybrid approach decreases the time the HAS services were unavailable, for all of the 10 trials, by a minimum of 58.28%, on average by 59.85%, and a maximum of 61.45%.

6.6 Conclusions

In this chapter, we have proposed a novel hybrid remote access scheme, which incorporates an adapted direct access approach (RHS-2) for the provision of quick communications for low security communications and a third party based approach (RHS-1) which provides the securest level of communications for critical applications and an increased level of information privacy for homeowners. The RHS-2 approach serves to provide communications for critical applications during DoS attacks, which disable the third party or prevent remote users from accessing

the third party. This proposed new hybrid remote access approach aims to increase the robustness of remote communications with HASs to withstand the effects of DoS attacks against third parties. Moreover, the proposed approach endeavours to provide the optimal combination of security and speed at all times.

The evaluation of the existing and proposed remote access approaches consists of three stages. Firstly, the existing direct, GHS, and proposed hybrid remote access approaches are tested and compared on the home automation test-bed, detailed in Chapter 5. The first research based performance analysis of the different remote access approaches identifies that the efficiency (speed of communications) differs for the different approaches. The direct access approach is the fastest of the four approaches analysed to login, share secure parameters and send three consecutive commands in all of the 10 trials, taking on average 2661ms (a minimum of 2604ms and a maximum of 2793ms). The proposed RHS-2 approach provides the second fastest performance in all of the 10 trials, a minimum of 19,8% (3189ms) slower, on average 20.59% (3209ms) slower, and a maximum of 20.80% (3215ms) slower. The GHS approach is the third slowest in all of the trials, being a minimum of 39.23% (3705ms) slower, on average 45.81% (3880ms) slower, and a maximum of 46.60% (3901ms) slower. The RHS-1 approach is by far the slowest in all of the 10 trials, being a minimum of 86.85% (4972ms) slower, on average 92.78% (5130ms) slower, and a maximum of 95.60% (5205ms) slower.

Secondly, a qualitative study shows that although the direct access approaches offer the best performance for homeowners, they provide the least security. Thirdly, an investigation of the vulnerability of remote access approaches to DoS attacks highlights the high vulnerability of third party based remote access approaches to DoS attacks. Hence, the evaluation results support the need for a hybrid remote access approach for a comprehensive remote access solution.

In all of the trials conducted, the third party based GHS and RHS-1 approaches allowed 0% of messages to reach their destination during an effective DoS flooding attack against the third party. The proposed hybrid approach is implemented on the same test-bed and shown to detect DoS attacks against the third party and switch communications from the securer RHS-1 approach to the RHS-2 approach allowing communications to continue, in all of the trials conducted. The

experiments show that the proposed hybrid approach decreases the time the HAS services were unavailable compared to the RHS-1 approach, in all of the 10 trials by a minimum of 62.34%, on average 63.75%, and a maximum of 65.19%. Moreover, compared to the GHS approach the proposed hybrid approach decreases the time the HAS services were unavailable, for all of the 10 trials, by a minimum of 58.28%, on average by 59.85%, and a maximum of 61.45%.

Chapter 7

Increasing WSN Resistance to Remote DoS Attacks

7.1 Background and Motivation

There are numerous approaches for protecting resource rich servers from DoS attacks, as discussed in Chapter 3. However, most DoS defence approaches perform two abstract functions (Mirkovic 2003). Firstly, DoS defences detect the onset of DoS attacks and attempt to distinguish between legitimate network traffic and network traffic arising from a DoS attack. Secondly, the defences attempt to mitigate any detected DoS attacks. The primary difficulty in dealing with DoS attacks arises from the difficulty in distinguishing between legitimate network traffic and network traffic from DoS attacks (Mirkovic 2003). Due to this difficulty, a percentage of attack traffic is misclassified by the existing defence approaches as legitimate traffic and allowed to reach the victim. Conversely, a percentage of legitimate traffic is misclassified as attack traffic and subjected to DoS attack countermeasures. As a result, to prevent defence measures from completely disrupting misclassified legitimate traffic, most defence measures perform rate limiting on suspected attack traffic, as discussed in Chapter 3. Rate limiting prevents the majority of traffic identified as attack traffic from reaching the victim,

however allows a small stream of suspected attack traffic to reach the victim, thus reducing the negative impact on misclassified legitimate traffic. Consequently, DoS defences do not effectively filter out all attack traffic during a DoS attack. A low-level stream of misclassified attack traffic and rate limited attack traffic reaches the victim. For example, as discussed in Chapter 3, one of the most effective DoS defence approaches identified from the research "D-WARD" claims to detect 99.4% of attack traffic (Mirkovic 2003), thus allowing 0.6% of attack traffic to reach the victim.

In terms of DoS defence for relatively resource rich computers, the existing defence approaches provide a satisfactory level of protection. The small amount of attack traffic reaching the victim is insufficient to cause a disruption to services for legitimate users. However, in terms of WSN based HASs where resources are intentionally limited to achieve the lowest cost possible, the low-level attack traffic reaching the home automation network poses a significant threat (Kumar et al. 2006). The low-level DoS attack traffic reaching the victim is sufficient to flood the home automation network's limited bandwidth resources and quickly exhaust the scarce, non-renewable, power sources of intermediate nodes. Moreover, low-level DoS attacks targeting the resources at the point of ingress between the home automation network and the Internet (Home Gateway) are sufficient to prevent remote users from communicating with the HAS, as identified from the literature review (see Chapter 3) and experimentally evaluated and confirmed later in this chapter.

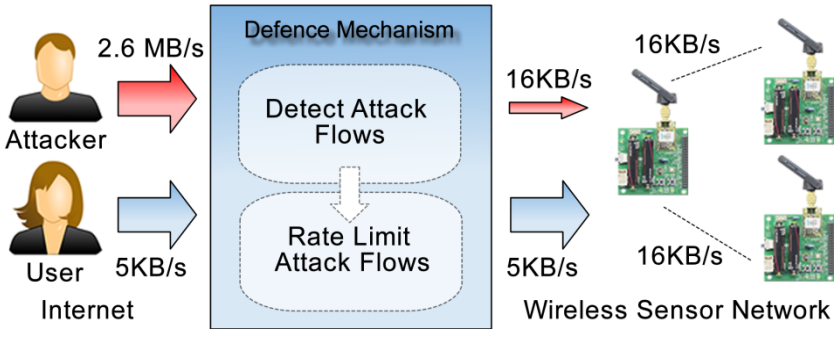

Figure 7-1: Existing DoS defence measure protecting a WSN

For example, Figure 7-1 depicts a user and attacker remotely communicating with a WSN. The WSN supports a maximum data rate of 16 KB/s. Let us assume that in this example the previously discussed D-WARD defence mechanism, which

is claimed to detect 99.4% of attack traffic, is employed. To exhaust the 16 KB/s of bandwidth provided by the WSN, the attacker needs to launch an attack of approximately 2.6MB/s. This level of an attack allows 16 KB/s of misclassified attack traffic to reach and disrupt the WSN, preventing local users from accessing the WSN in a timely manner. Moreover, such an attack overwhelms the home gateway and prevents remote users from accessing the WSN for the duration of the attack.

As discussed in Chapter 3, the home automation test-bed adopts the ZigBee WSN standard based on the IEEE 802.15.4 low data rate WSN standard. Table 7-1 summarises the different data rates supported by the IEEE 802.15.4 standard and the respective theoretical attack size required to exhaust the available bandwidth of an unprotected IEEE 802.15.4 based WSN, and an IEEE 802.15.4 WSN protected by D-WARD, which filters 99.4% of attack traffic.

Table 7-1: Attack size required to exhaust the available bandwidth of an unprotected and protected ZigBee based WSN

IEEE 802.15.4 Frequency Band	Available Bandwidth (Maximum Data Rate - KB/Sec)	Theoretical Size of Attack Required to Exhaust the Available Bandwidth (KB/Sec)	
		No Defences	D-Ward DoS Defences
868 – 870 MHz	2.4	2.4	406.9
902 – 928 MHz	4.9	4.9	813.8
2.4 GHz	30.5	30.5	5086.3

Table 7-2: Available broadband speeds in the 2009 UK market

Broadband Speed (Mb/s)	Broadband Speed (KB/s)
2	256
4	512
8	1024
12	1536
20	2560
50	6400

Table 7-2 highlights the broadband speeds available in the UK during 2009. Most ISP's provide an 8Mb/s broadband service, which implies that a sufficiently large DoS attack can be launched against a significant number of homes in the UK to exhaust the available bandwidth of all unprotected ZigBee networks. Moreover, an attack against a significant number home in the UK with DoS defences in place can exhaust the available bandwidth of all connected ZigBee networks, except those

adopting the 2.4 GHz frequency. Furthermore, in countries where broadband speeds are more developed than the UK and in the near future, when 50Mb/s broadband connection speed is widely adopted in the UK, all ZigBee WSNs will be vulnerable to remote low-level DoS attacks, even if the existing DoS defence approaches are adopted. Additionally, for low data rate WSNs, such as those based on the IEEE 802.15.4 standard, low cost and low energy consumption are fundamental design principles. Consequently, future developments leading to the increase in the data rate of WSNs cannot be relied on to provide protection for WSN based HASs (Raymond et al. 2008) from more aggressive low level DoS attacks as broadband speed increases further.

The objective of this chapter is to introduce the design, implementation and evaluation of a novel third party based approach for mitigating low-level DoS attacks targeted at WSN based HASs and the respective remote access infrastructure. The evaluation includes assessing the effectiveness of existing DoS defence approaches for protecting WSN based HASs and identifying the effects of low-level attack traffic, which existing defence mechanisms allow to reach the victim, on WSN based HASs. Furthermore, the effectiveness of the proposed defence approach in unison with the existing defence approaches for combating low-level DoS attacks is investigated. The work presented in this chapter is published in (Gill & Yang 2009b).

7.2 Proposed Defence Approach

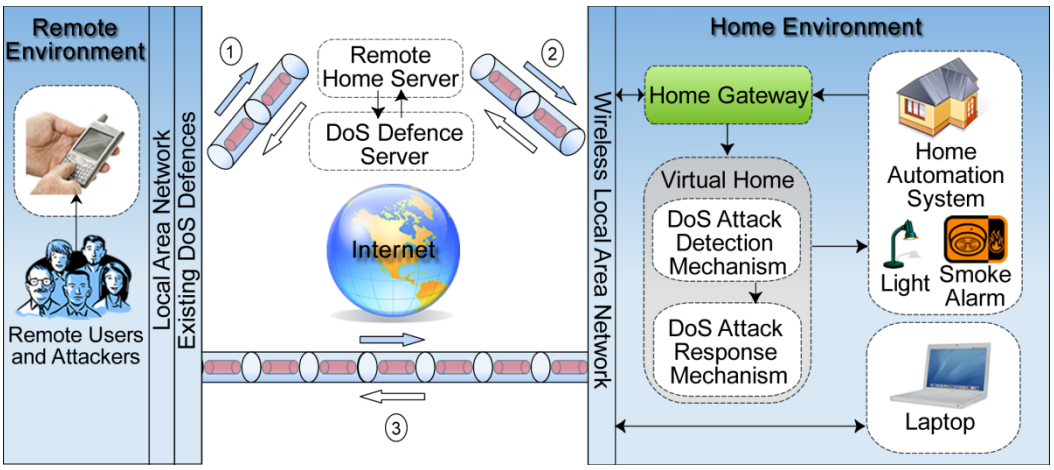

Figure 7-2: Low level DoS defence approach for protecting WSN based HASs

This section introduces the design of a novel defence approach for supplementing the existing DoS defence approaches and providing improved protection for resource limited WSN based HASs from low-level DoS attacks.

The proposed DoS defence approach consists of three entities, the "Virtual Home" (VH), "Remote Home Server" (RHS), and "DoS Defence Server" (DDS), as depicted in Figure 7-2. The VH is designed to filter out all attack traffic including attack traffic misclassified as legitimate traffic and rate limited attack traffic allowed through by existing DoS defences, consequently preventing the attack traffic from reaching the WSN based HAS. Hence, resolving the threats to the WSN from low-level attack traffic flooding the WSN. Furthermore, the VH is responsible for detecting low-level DoS attacks and providing an appropriate response. The VH incorporates a DoS attack detection mechanism and a DoS attack response mechanism to achieve this objective. The virtual home's attack detection mechanism works in unison with the RHS's DDS to selectively deal with DoS attacks. The RHS and the DDS help overcome the threat of low-level DoS attacks targeted at the point of ingress between the Internet and HAS (Home Gateway). These elements and their placement in the home automation architecture are described in more detail in the remainder of this chapter.

7.2.1 Virtual Home - DoS Attack Detection Mechanism

The remote communications architecture employed in the proposed system encrypts all communications between the remote user and the HAS. End-to-end encryption is employed to protect the homeowner's privacy from malicious users, see Chapter 6 for more details. This has the advantage, in terms of DoS prevention, that all incoming attacks can be detected with 100% accuracy, unless the attacker has access to the secret key used for encryption. This allows the VH to filter out all non-legitimate traffic at the point of ingress between the HAS and Internet before the attack traffic reaches the WSN based HAS. Consequently, preventing the earlier discussed threats faced by the HAS from low-level DoS attacks such as exhaustion of WSN bandwidth and energy resources. Existing DoS defences do not employ encryption for the detection of DoS attacks because the overheads associated with encrypting all communications even within a home network are excessive. However, the relatively low data rate home automation communications can use the

encryption approach with little impact on performance. This is due to the positioning of the VH, which allows for communications destined for the HAS to be selectively filtered, this is discussed further in Section 7.2.4.

The DoS attack detection mechanism monitors the following conditions to detect potential DoS attacks:

- Unencrypted incoming attack packets generate decryption errors.
- Encrypted packets encoded with an incorrect encryption key fail to decrypt successfully.
- Replayed packets, after a session has expired, fail to decrypt successfully.
- Replayed packets, before a session has expired, generate message freshness errors.

The DoS attack detection algorithm monitors to see if any of the conditions arises. The DoS attack detection algorithm repeatedly cycles through the rule below, which is based on the previously identified attack characteristics. If any of the characteristics are detected and the rule is satisfied, a DoS attack is assumed to have started.

$$\text{If } (DE + DF + RM) > 0 : \text{FLAG}$$

Table 7-3: Key system parameters

Parameter	Definition	Default Value
DE	Number of decryption errors in a given minute.	0
DF	Number of decryption failures in a given minute.	0
RM	Number of replayed messages in a given minute.	0

Once the rule is satisfied, a flag is set. Table 7-3 provides a summary of the DoS attack detection mechanism parameters. Once the flag has been set no immediate action is taken to mitigate the potential attack. Instead, a message is sent to the RHS to initiate an analysis of the home gateway to identify with greater certainty if there is a DoS attack underway. If on receipt of the analysis results from the RHS, the

analysis indicates an attack is underway and is significantly effecting the communication of legitimate users the DoS attack response mechanism is activated to mitigate the attack. If the analysis indicates that no attack is underway or that an attack is underway, however the average connection latency for the HAS is within acceptable limits the DoS detection mechanism continues to monitor the situation. If the RHS fails to respond to an analysis request this may indicate that there is an active DoS attack of sufficient strength to block the RHS from communicating with the home gateway. Alternatively, the RHS may be offline due to a technical fault. In either case, the DoS Attack Response Mechanism is activated. The objective of the activation of the DoS attack response mechanism is to resolve the earlier identified threats to the home gateway from low-level DoS attack traffic that may prevent remote users from accessing the home automation network and maintain effective remote communications. The pseudo code for the virtual home is depicted in Figure 7-3 (a) and (b).

7.2.2 RHS - DoS Defence server

The DoS analysis requests received by the RHS are routed to a dedicated DDS. A dedicated DDS is employed to prevent any service impact on legitimate users using the RHS for communication purposes. The role of the DDS is to emulate a legitimate home automation user wishing to remotely access a HAS and calculate the average connection latency. The DDS calculates the latency, as a value of service degradation, of the relevant home gateway through repeatedly connecting to the HAS from a simulated mobile device. An average latency value is calculated for all the connection attempts, and if the service degradation exceeds a predefined threshold value set by the respective homeowners a message is sent to the respective VH to respond to the attack. Otherwise, a message is sent to the VH to take no action and continue to monitor the situation.

7.2.3 Virtual Home - DoS Attack Response Mechanism

The purpose of the DoS attack response mechanism is to act on the connection latency analysis performed by the DDS to mitigate detected DoS attacks and maintain effective communications between remote users and the HAS, overcoming any low-rate DoS attacks against the home gateway. The proposed DoS

attack response mechanism makes use of the RHS-1 and RHS-2 connection approaches discussed in Chapter 6. Firstly, under normal conditions, where performance is of a greater concern than security the RHS-2 approach is adopted, allowing remote users to directly form a secure connection with the HAS, as depicted in Figure 7-2 interconnection (3).

Secondly, under DoS attack conditions the DoS attack response mechanism switches from the RHS-2 connection approach to RHS-1 connection approach. A message from the DDS triggers the VH to disable all support for incoming connections to the HAS and create an outgoing connection to a third party. The remote users connect to the third party and create a secure tunnel between themselves and the HAS (See Figure 7-2, interconnection (1) and (2)). Experiments have shown that the RHS-1 approach is 48.13% slower than the RHS-2 approach (See Chapter 6). However, during a DoS attack the effect of the DoS attack response mechanism disabling support for all incoming connections is to terminate all incoming DoS attack connections. Only legitimate users will be able to switch to the RHS-1 connection approach, authenticate with the third party and establish a mediated secure connection with the HAS. During a DoS attacks, the switch over from the RHS-2 approach to the RHS-1 approach will also disconnect previously authenticated connections, requiring legitimate users to reconnect using the RHS-1 connection approach. However, during a DoS attack the service quality for previously authenticated connections will also be degraded, so this solution offers an acceptable compromise. All communications to the home automation network must traverse the outgoing connection from the HAS to the third party. Direct connection requests from an attacker to the HAS are immediately dropped at the local network, shifting the focus and bottleneck of the attack away from the WSN based HAS. Therefore, the attacker has to launch a considerably larger DoS attack against the relatively resource rich local area network to be effective.

The DoS attack response mechanism switches back to the RHS-2 approach, after a user-defined period and executes the DoS attack detection mechanism. If the DoS attack is over, the DoS attack response mechanism returns to using the RHS-2 communications approach. If the DoS attack has not ended the system returns to the RHS-1 communication approach. This check is performed periodically to ascertain

when the DoS attack has ended and the RHS-1 approach can be resumed. The user-defined period between checking if a DoS attack has ended, is a compromise between a shorter delay, which generates more interruptions for the active users, and a longer delay, which will lead to users using the slower connection approach (RHS-1) for longer than is required. If the home gateway cannot establish a connection to the RHS (RHS-1 mode), a technical fault with the RHS is assumed and RHS-2 mode of communications is resumed. The approach helps provide users with the optimal security and service combination at all times. The pseudo code for the virtual home is depicted in Figure 7-3 (a) and (b).

7.2.4 Virtual Home Placement

As discussed in Chapter 3, existing systems designed to handle DoS attacks are predominantly located at the edges of victim networks. Recently new systems have been proposed that reside at distributed locations across the Internet or at the edge of victim networks. These approaches take a cart-blanche approach to filtering network traffic. Existing approaches are designed to filter all Internet traffic passing between two points. The proposed VH is positioned at the edge of the WSN based HAS. As depicted in Figure 7-2, the VH is installed on a home gateway, which is located between the edge of the home automation network and the homes local network used to provide access to the Internet. This point is the crucial bridge between other networks and home automation network. All the inbound or outbound home automation data traverses this connection. Hence, the location of the VH allows for the precise monitoring and filtering of home automation data, whilst allowing data destined for other networks to be monitored by existing DoS defence approaches or go unmonitored. This is depicted in Figure 7-2, a laptop user can directly connect to the Internet and be sufficiently protected by existing DoS defences without being affected by the virtual home.

This approach allows for the selective encryption of all home automation communications and provides total protection for the HAS. Unless the home's secret key is known by an attacker, no attack traffic is sent across the resource constrained WSN. In the worst-case scenario the resources of the VH may be exhausted, rendering the remote users without access to the HAS, however local users and home automation devices will be unaffected.

Virtual Home Pseudo Code

Step 1. Call the function to analyse the decryption results every minute for the whole time the application is active.

```
Timer(60000);

Function Timer(Delay){

        analysis();
        Timer(60000);
}
```

Step 2. The decryption function is called whenever there is data in the systems input buffer. All replayed messages, decryption failures and decryption errors will be recorded during this process.

```
Function decrypt(){

        rawMessage = (inputBuffer);
        message = decrypt(rawMessage);

        if(message.nonce not correctly incremented){
                nonceReplay = nonceReplay + 1;
        } else if(message.decryption = fail){
                decryptionFailure = decryptionFailure + 1;
        }else if(message.decryption = error){
                decryptionError = decryptionError  + 1;
        }else if(message.DDSAnalysisResult){
                switch(message.DDSAnalysisResult);
        }
}
```

Step 3. This function is executed every 60000ms, if a potential DoS attack is detected a message is sent to the DDS to perform an analysis of the WSN based HAS connection latency.

```
Function analysis(){

        int Flag = 0;

        if(nonceReplay > 0){
                Flag = 1;
                nonceReplay = 0;
        }if(decryptionFailure > 0){
                Flag = 1;
                decryptionFailure = 0;
        }if(decryptionError > 0){
                Flag = 1;
                decryptionError=0;
        }if(Flag == 1){
                Send(WSN based HAS analysis request to DDS);

        }
}
```

Figure 7-3: (a) Virtual home pseudo code

Virtual Home Pseudo Code

Step 4. This function chooses which communication approach the WSN based HAS is currently using.

```
Function Switch(message.DDSAnalysisResult){
        if(message.DDSAnalysisResult equals "switch"){
                Switch to using the third party RHS-1 Approach();   //Stop support for incoming
                connections
        }else if (message.DDSAnalysisResult equals "do not switch"){
                Do not switch communications approach();            //Continue using direct
                RHS-2 approach
        }
}
```

Figure 7-3: (b) Virtual home pseudo code

7.3 Implementation of the Proposed Defence Approach

This section describes in detail the implementation of the proposed low-level DoS attack defence approach, discussed in the previous section, and the development of an attack tool designed to launch low-level DoS attacks and test the proposed defence approach. Figure 7-4 provides an overview of the implementation architecture of the proposed defence and attack tool. Due to the close integration of the proposed defence approach and the previously discussed remote access approaches (RHS-1 and RHS-2), a number of the implemented components of the

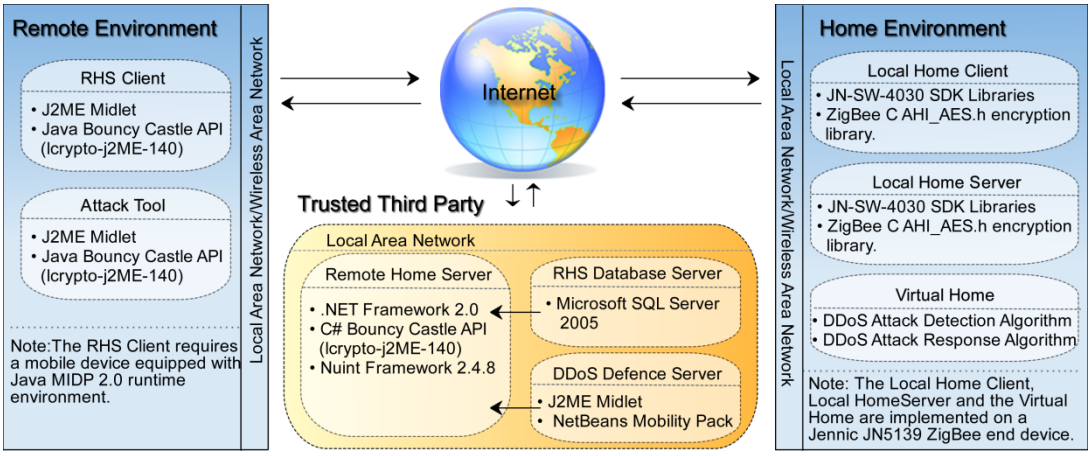

Figure 7-4: Low level DoS defence approach system architecture

proposed defence strategy overlap with those developed for other approaches and are consequently described in greater detail in Chapters 5 and 6.

As depicted in Figure 7-4, the DoS defence strategy consists of four components. Firstly, the RHS client is installed on the user's mobile phone, which

provides a graphical interface and allows users to initiate a RHS-1 or RHS-2 connection with the HAS. Secondly, the RHS is installed on the resource rich servers of a trusted third party and takes part in the RHS-1 and RHS-2 communication approaches. Thirdly, the DDS is hosted alongside the RHS and is responsible for calculating the average connection latency for a HAS, to help identify HASs under a DoS attack. Fourthly, there is the home gateway, which hosts the VH and provides the DoS detection and resolution mechanisms. Additionally, an attack tool has been developed to launch low-level DoS attacks against the home automation test-bed to validate the effectiveness of such attacks against WSNs and to evaluate the implemented defence approach.

This section presents the implementation of the proposed components new to the low-level DoS defence approach or those modified from previous approaches including the DDS and attack tool. For information regarding the implementation of the RHS Client, Remote Home Server, and Home Gateway please refer to Chapter 6. Moreover, for more information regarding the implementation of the home automation test-bed please refer to Chapter 5.

7.3.1 DoS Defence Server

A standard laptop hosts the DDS. The DDS consists of a Java midlet and a simulated mobile phone. The NetBeans mobility pack 5.5 is used to simulate a mobile phone on which the midlet runs. The midlet attempts to initiate a predefined number of connections to the home gateway and calculate the average connection latency. Moreover, the DDS is pre-programmed by users with a predefined latency threshold. Once the connection latency threshold is passed, the midlet creates a TCP connection to the RHS and advises the respective HAS to change communication approaches from RHS-2 to RHS-1. Otherwise, the DDS informs the respective HAS to continue using the RHS-2 communications approach. The pseudo code for the DDS is depicted in Figure 7-5.

Distributed Denial of attack Defence Server (DDS) Pseudo Code

Step 1. Call the function to analyse the respective homes connection latency

```
Function latencyCheck(){

        long averagelatency = 0;
        long sumLatency = 0;
        int NumberofChecks = 50;
        int counter = 0;
```

Step 2. Emulate a mobile user by connecting to the respective WSN based HAS and summing the connection latency.

```
        while(counter < NumberofChecks){
                Thread.sleep(1000);  //adds a 1000 ms delay between connection attempts
                long startTest = System.currentTimeMillis();
                long endTest = send(message);  //The send message returns the system time when
                the
                                                //send completes, including connection times.
                sumLatency = sumLatency + (endTest-startTest);
                counter++

        }
```

Step 3. Calculate the average connection latency and compare the result with the predefined latency threshold value and inform the WSN based HAS of the findings.

```
        averageLatency = (sumLatecy/NumberofChecks);
        If(averageLatency >= 3000){
                Send(switch message to WSN based HAS);
        }else{
                Send(latency below threshold message to WSN based HAS);
        }

}
```

Figure 7-5: Distributed denial of attack defence server pseudo code

7.3.2 Attack Tool

A Java based attack tool was developed to evaluate the effectiveness of low-level DoS attacks against WSNs protected with, existing DoS defences, and WSNs protected with existing defences and the proposed defence approach.

Attacker Pseudo Code

```
Step 1. Call the attack function to begin the attack
    Function Attack (String attackType)
    {
Step 2. Based on the attack type requested, generate and initialise the attack data
    String attackMessage = "";
        If(attackType == "UnencryptedDataAttack"){
            attackMessage = UnencryptedDATA;
        }
        If(attackType == "IncorrectlyEncryptedDataAttack"){
            attackMessage = IncorrectlyEncryptedData;
        }
        If(attackType == "CapturedDataReplayAttack"){
            attackMessage = ReplayedEncryptedData;
        }
Step 3. Commence the attack until the attacker decides to halt the attack
        Boolean attackStatus = true;
        while (attackStatus) {
            Open connection to victim (IP Address, Port)
            Send(attackMessage);
            Close connection to victim(IP Address, Port)
            If(stopAttack){
                attackStatus = false;
            }
        }
    }
```

Figure 7-6: Attack node pseudo code

To test the effectiveness of low-level attacks targeted at the WSN based HAS with the existing DoS defence approaches, the attack tool sends unencrypted data to the home gateway, which is subsequently forwarded across the WSN to the victim device. Additionally, to test the effectiveness of the proposed defence approaches for protecting the WSN based HAS from attacks targeting the home

gateway in an attempt to prevent remote users from effectively accessing the system, the attack tool launches an application level TCP attack against the WSN. The attack tool relies on the fact that the home gateway allows a temporary TCP connection to be formed to receive authentication data. If the connection remains idle after the initial connection and no authentication data is received the connection is rejected. However, the attack tool attempts to exhaust the home gateways TCP connection authorisation mechanism, by initiating TCP connections and sending message replays of legitimate data, data encrypted with a random key and unencrypted data. The home gateway has to validate this authentication information before the active connection is dropped. Due to the resource limited nature of the home gateway legitimate users may not be able to connect while the home gateway is authenticating a large number of connections. The Bouncy Castle API provides the attack tool with the necessary encryption functionality to launch the attacks. The pseudo code for the attack tool is depicted in Figure 7-6.

A simple simulation of the D-WARD defence tool is implemented alongside the attack tool. The simulation rate limits the attack traffic generated and stops 99.4% of the attack traffic from being transmitted.

7.4 Evaluation

The evaluation of the proposed low-level DoS defence approach consisted of two stages. Firstly, the effectiveness of low-level DoS attacks, that existing defence mechanisms allow to reach the victim, on WSN based HASs was investigated. Moreover, the effectiveness of the proposed approach for protecting the WSN based HAS test-bed from disruptions, due to low-level DoS attacks was investigated. Secondly, the effectiveness of the proposed approach for protecting the Home Gateway from low-level DoS threats, seeking to disrupt the communications of remote users, was investigated.

7.4.1 Analysis of low level DoS attacks on WSN based HASs

The WSN based HAS test-bed was converted into a star topology configuration. The attack tool was used to send attack data to the WSN based HAS from across the local network, through the home gateway to the victim. A simulation of the D-

WARD attack tool removed 99.4% of received attack traffic before reaching the WSN at the source network. Ten trials of the experiment were conducted. As depicted in Figure 7-7, at the start of the experiment no attack data was sent to the WSN. The average packet loss rate for all of the 10 trials during normal communications between a local device and the victim device was measured as a 2.5% average packet loss rate, with a minimum packet loss rate of 0%, and a maximum packet loss rate of 3.12%. The attack rate was then increased. For each attack rate, the experiment was repeated 10 times and the average packet loss-rate calculated. The attack rate stated in Figure 7-7 and 7-8 refers to the effective attack rate that reaches the WSN after the existing defence approaches have removed 99.4% of attack traffic. It was found that for an attack rate of less than 32 packets per minute (ppm) the average ppm loss rate was 3.1%, with a minimum ppm loss rate of 0% and a maximum ppm loss rate of 3.12%. However, when the attack rate was increased to 50ppm, on average 26.9% (a minimum of 18.75% and a maximum of 34.38%) of packets between users on the WSN and victim were lost. As the attack rate was further increased, the ppm loss rate also increased, for all of the 10 trials. At an attack rate of 128ppm, an average of 73.5% (a minimum of 68.75% and a maximum of 81.25%) of packets were lost, rising to an average packet loss rate of 86.25% (a minimum of 84.38% and a maximum of 93.75%) for an attack rate of 256ppm. It should be noted that for all of the 10 trials, as the attack rate was increased, the percentage ppm loss rate also increased. The packet size during the attack was 133 bytes. Consequently, the experiment suggest that an effective attack of approximately 567 (256/60 * 133) bytes per second is sufficient to seriously disrupt communications on the WSN based HAS, with an average packet loss rate of 86.25%. The attack size required to allow 567 bytes per second to bypass the existing defences and reach the WSN at the attacker end is 92KB/s. This implies that a far smaller low-level DoS attack can have a far greater effect on the WSN than the earlier calculated theoretical attack size required to exhaust the WSN communication bandwidth. In the case of the experiments, the WSN based HAS test-bed adopted the 2.4 GHz frequency range. As discussed earlier, the theoretical effective attack size required to exhaust the available bandwidth is 30.5 KB/s with an initial attack size of 5086 KB/s at the attacker end, before the existing DoS defences rate limit the attack traffic. This implies that the actual maximum bandwidth available is less than the theoretical value stated, or/and that other

underlying factors are affected by the low level DoS attack at other levels of the WSN stack. It can be surmised that the utilisation of the theoretically available bandwidth is considerably lower, when multiple nodes compete for access to the communications channel. Moreover, the input buffer size of the WSN nodes may be insufficient to handle such large data rates leading to packets being dropped. Unfortunately, the lower levels of the ZigBee and IEEE 802.15.4 stack are not accessible for testing with the available equipment. Consequently, the underlying factors affected by the low-level DoS attack cannot be investigated further.

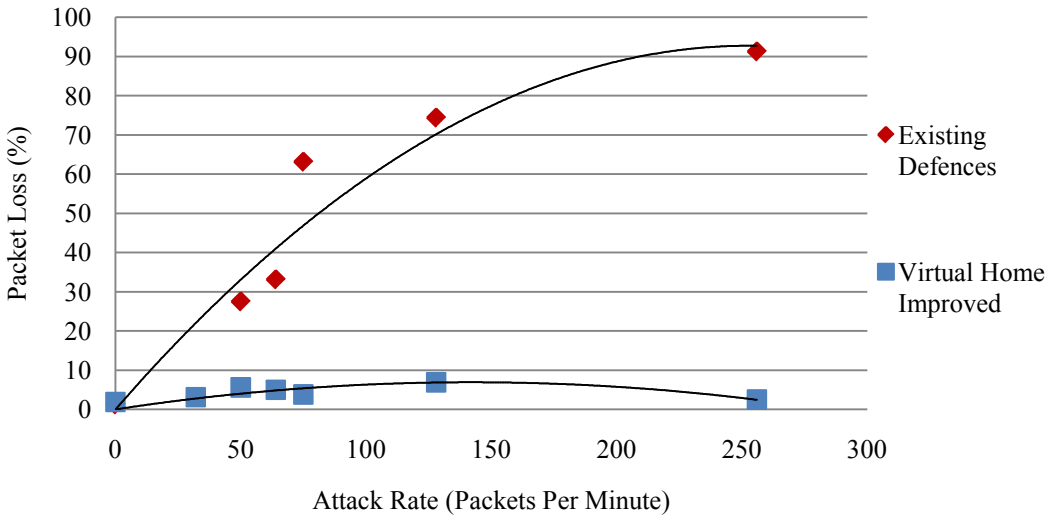

Figure 7-7: Average percentage packet loss under different levels of DoS attacks in a ZigBee network using a star topology

The experiment was repeated with the addition of the proposed defence approach integrated with the WSN based HAS. Figure 7-7 shows that the VH effectively prevented the attack data from reaching and disturbing the WSN. Figure 7-7 shows during the remote low-level DoS attacks, the average packet-loss rate remained at a minimum of 1.9%, on average 4.11%, and at a maximum of 6.9%. The addition of the proposed defences, alongside the existing defences, in this experiment reduced the percentage packet loss on the WSN, caused by the DoS flooding attack for all of the trials. The minimum reduction recorded was of 84.70% for all of the 10 trials, with an average reduction of 91.13% and a maximum reduction of 95.6% compared to the same trials, with only the existing D-WARD defence in place.

The WSN based HAS test-bed was then configured using a partially connected mesh topology. In such a topology, the end devices have one parent node as in the star topology. However, the partially connected mesh topology contains routers that can be used to send communication through multiple routes across the WSN. Figure 7-8 illustrates the findings from the experiments.

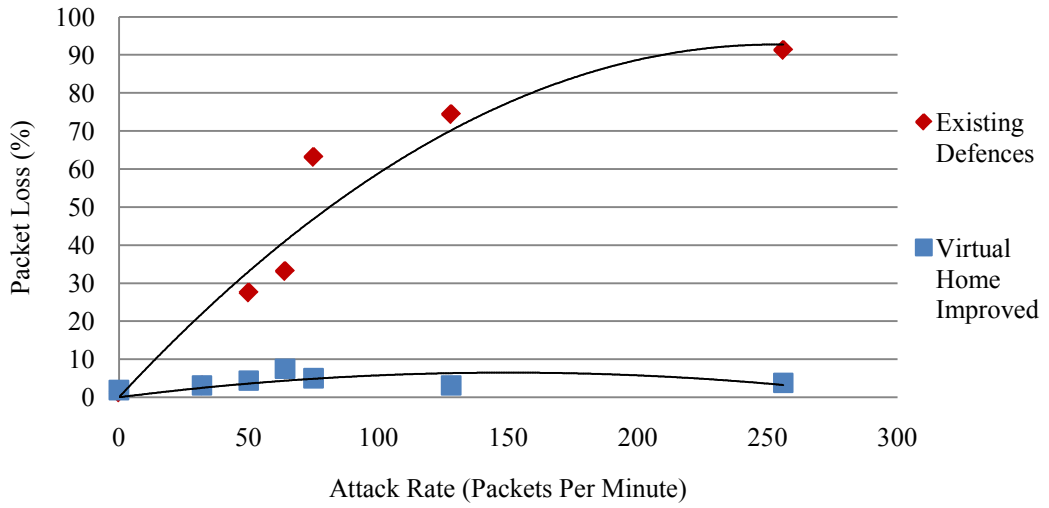

Figure 7-8: Average percentage packet loss under different levels of DoS attacks in a ZigBee network using a partially connected mesh topology

As depicted in Figure 7-8, at the start of the experiment no attack data was sent to the WSN. The average packet loss rate for all of the 10 trials during normal communications between a local device and the victim device was measured as a 1.25% average packet loss rate, with a minimum packet loss rate of 0%, and a maximum packet loss rate of 3.12%. The attack rate was then increased. For each attack rate, the experiment was repeated 10 times and the average packet loss-rate calculated. It was found that for an attack rate of less than 32 packets per minute (ppm) the average ppm loss rate was 3.1%, with a minimum ppm loss rate of 0% and a maximum ppm loss rate of 6.25%. However, when the attack rate was increased to 50ppm, on average 27.5% (a minimum of 19.25% and a maximum of 35.00%) of packets between users on the WSN and victim were lost. As the attack rate was further increased, the ppm loss rate also increased, for all of the 10 trials. At an attack rate of 128ppm, an average of 74.38% (a minimum of 70.75% and a maximum of 83.75%) of packets were lost, rising to an average packet loss rate of 91.25% (a minimum of 85.75% and a maximum of 94.75%) for an attack rate of

256ppm. It should be noted that for all of the 10 trials, as the attack rate was increased, the percentage ppm loss rate also increased.

As depicted and analysed, the results of the 10 trials for both the star and partial mesh configuration of the WSN based HAS, indicate that the findings are consistent. This implies that the limiting factors, which are affected by the low level DoS threat resides on the victim nodes parent or at the victim node itself. Although the mesh network vastly increases the routes to the victim node, the bottleneck at the victim's parent node or at the victim, results in no improvement in the WSNs resilience to low level DoS attacks. The addition of the VH, as in the star topology configuration of the WSN based HAS, provides effective protection for the network and prevents any attack data from reaching the WSN, during all of the 10 trials. This results in no noticeable abnormal loss of packets during the remote low-level DoS attack, with the average packet-loss rate remaining at a minimum of 1.9%, on average 4.17%, and at a maximum of 7.5%. The addition of the proposed defence, alongside the existing defences, in this experiment reduced the percentage packet loss on the WSN caused by the DoS flooding attack, for all of the trials. The minimum reduction recorded was of 78.34% for all of the 10 trials, with an average reduction of 91.20% and a maximum reduction of 95.60% compared to the same trials, with only the existing D-WARD defence in place.

7.4.2 Analysis of low level DoS attacks on the home gateway

The previously discussed attack tool was used to generate TCP attack packets (115 bytes per connection attempt), targeted at the home gateway. The attack tool targeted an unprotected home gateway at varying rates between 0 and 1200 attacks per minute. Each attack rate was trialled 10 times. The results showed a minimum latency of 513ms, an average latency of 530ms, and a maximum latency of 581ms for the successful creation of a TCP connection during the presence of no attack traffic, as depicted in Figure 7-9. A noticeable change in average latency can be seen at an attack rate of 429 attacks per minute reaching a minimum latency of 1679ms, an average latency of 1802ms and a maximum latency of 1870ms. Figure 7-9 shows that as the attack rate is increased the average latency goes up correspondingly. At 1090 attacks per minute, a relatively small attack rate, there is a minimum latency of 7130ms, an average latency of 7431ms and a maximum latency

of 7942ms. This level of attack, although relatively low, would lead to a substantial degradation in service for a system using the RHS-2 communications approach.

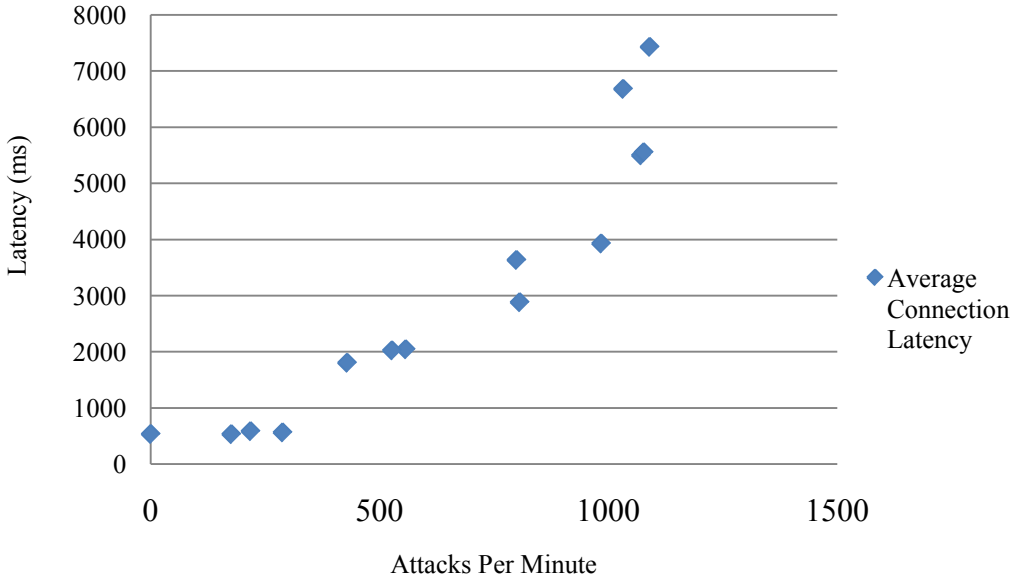

Figure 7-9: Connection latency during differing rates of attack

Figure 7-10 shows the number of connection failures before a successful connection could be established, for different attack rates. As depicted, no failed connection attempts were detected during normal operations when no attack was underway, during any of the trials. As in the previous experiments, at 429 attacks per minute a minimum of 21 connection attempts, an average of 37 connection attempts, and a maximum of 38 connection attempts were recorded before a successful connection. During a 1090 attacks per minute period a minimum of 78 connection attempts, an average of 101 connection attempts, and a maximum of 106 connection attempts were necessary to form a successful TCP connection.

From the analysis of connection latency during the attacks against an unprotected home gateway, 3 seconds was chosen as the threshold value an attack would have to reach before the DDS should trigger a response. The proposed virtual home and DDS were integrated into the previous experiment setup. Next, the proposed approach was subjected to 799 attacks per minute (the lowest attack rate which is shown to cause a disruption on the WSN based HAS, from the previous experiments) to the highest attack rate that could be generated of 2300 attacks per

minute. The attacks were repeated ten times as part of ten trials. The average results from which are illustrated in Figure 7-11 and 7-12 respectively.

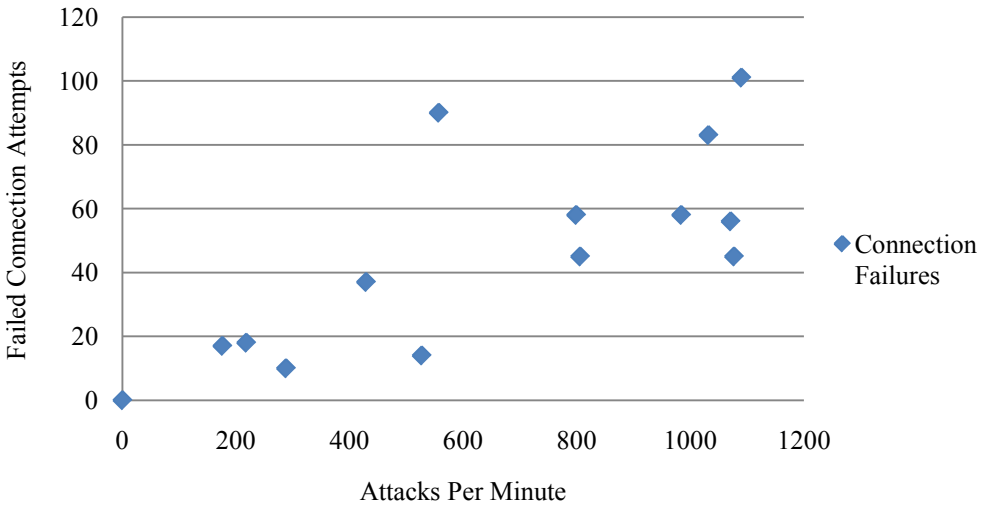

Figure 7-10: Failed connection attempts before a successful TCP connection is established

Figure 7-11 shows that from the onset of an attack (13:33) the average latency escalates quickly from 680ms to 3500ms (the minimum latency escalates from 510ms to 3316ms and the maximum latency escalates from 863ms to 3605ms). At this point, the virtual home detects encryption errors and message replays indicating a potential attack and requests the DDS to perform a check. The DDS performs a check and requests the Virtual Home to switch from RHS-2 to RHS-1. This all occurs within a three-minute interval (13:33-13:35 inclusive), in the case of all of the trials. Once the switch from mode RHS-2 to RHS-1 has occurred (13:36) the protected HAS average connection latency falls to 1515ms (the protected HAS connection latency for the ten trials falls to a minimum of 1478ms and a maximum latency recorded of 1536ms). The average latency for communications is higher for approach RHS-1 than for RHS-2. Hence, the higher latency after the attack starts and the RHS-1 mode is adopted, compared to before the onset of the attack, when using RHS-2 mode. After a period of 5 minutes (13:36 – 13:40 inclusive) in RHS-1 mode the attack was stopped. For the experiment 5 minutes was chosen as the user defined period the VH would switch back approaches (RHS-1 to RHS-2) and check if the DoS has ended. Consequently, as depicted, after 5 minutes the VH switches the connection from RHS-1 to RHS-2 mode and requests the DDS to perform a check to see if the DoS attack has ended. In the experiment, the attack had ended so

the VH continues to operate using the RHS-2 communication approach. The average latency after the attack returns to levels detected before the attack (a minimum of 498ms, an average of 617ms, and a maximum of 722ms).

The experiment was repeated (see Figure 7-12) and the home gateway was subjected to the largest attack rate that could be produced using the apparatus of 2300 attacks per minute. Again the experiments were repeated ten times, to form ten trials. Before the attack (14:30) the average latency recorded was 819ms (the minimum latency was 587ms and the maximum latency was 894ms). The attack was started (14:32) and the average latency quickly increased to 17361ms (the minimum latency for the ten trials was 16453ms and the maximum latency was 18020ms). As in the previous experment the attack detection and response mechanism took approximatly three minutes to operate, in the case of all of the ten trials. The comunication latency for the protected home gateway dropped quickly afterwards to an average 1580ms (a minimum latency of 1409ms and a maximum of 1716ms) consistent with operating in RHS-1 mode. The non protected home gateway continued to incur an average latency of 17361ms (a minimum latency of 13459ms and a maximum latency of 18471ms) until the end of the attack.

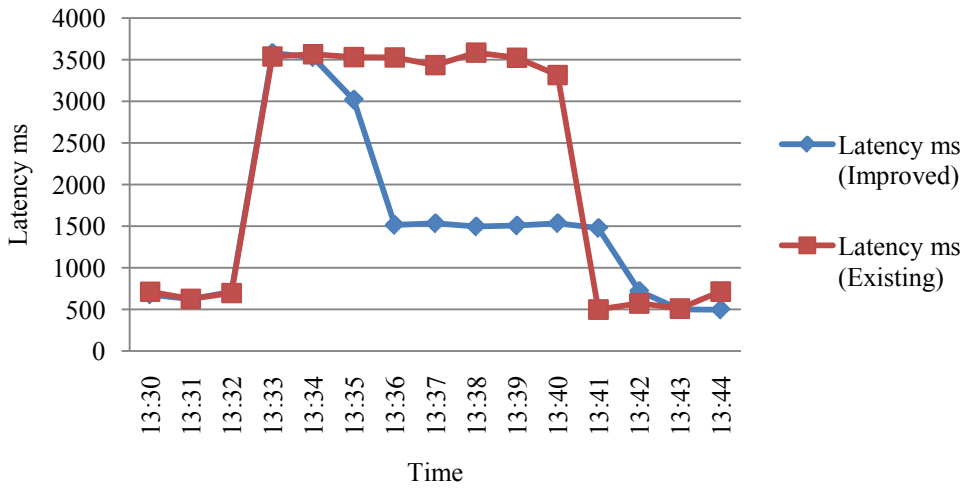

Figure 7-11: Virtual home in operation during 799 attacks per minute DoS attack

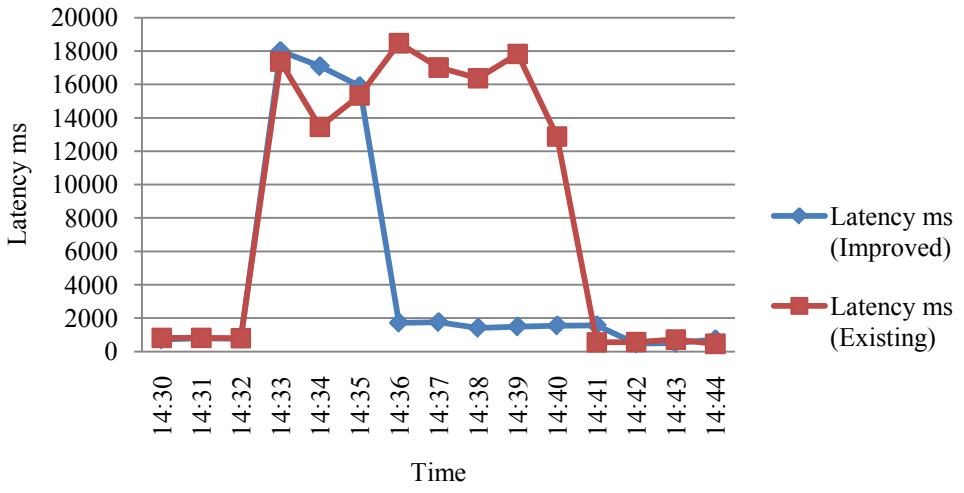

Figure 7-12: Virtual home in operation during 2300 attacks per minute DoS attack

Although at this level of attack the latency rate was not as stable as experiments under lower levels of attack, the attack was stopped after 5 minutes of operation in RHS-1 mode. As with the previous experiment, 5 minutes was chosen as the user-defined period the VH would use for switching back approaches (RHS-1 to RHS-2) and checking to see if the DoS attack has ended. Consequently, as depicted, after 5 minutes the VH switches the connection from the RHS-1 to RHS-2 communication mode and requests the DDS check if the DoS attack has ended. The average latency measured after the attack returned to levels detected before the attack (a minimum of 545ms, an average of 620ms, and a maximum of 714ms).

It should be noted that in the case of all of the ten trials, the proposed approach always resulted in a lower connection latency for both sets of experiments. In the experiment with a 799 attacks per minute rate, the proposed approach resulted in a minimum reduction in connection latency of 56.11%, an average reduction of 56.71%, and a maximum reduction of 57.77%. In the experiment with a 2300 attacks per minute rate, the proposed approach resulted in a minimum reduction of 90.14%, an average reduction of 90.90%, and a maximum reduction of 91.88%. This suggests that the proposed approach provides a greater reduction in the connection latency experienced by remote users during larger DoS flooding attacks, although more experimentation is required in future work to confirm this using apparatus capable of generating larger DoS flooding attacks.

7.5 Conclusions

This chapter has identified a new type of low-level DoS attack against WSN based HASs. It has been shown that existing DoS defence approaches do not provide sufficient protection for WSNs against low-level DoS attacks that originate from relatively resource rich coexisting networks, at the point of ingress between the WSN and local network. It has been shown that a large DoS attack can be executed that will allow a sufficient amount of attack traffic to penetrate existing DoS defences to cause a serious disruption to communications on the WSN. Moreover, low-level DoS attacks that target the home gateway of WSN based HASs have been shown to disrupt the communications of remote users attempting to remotely access the WSN based HAS. A new approach, incorporating a virtual home and DoS Defence Server has been proposed to tackle low-level DoS attacks and experimentally shown to help increase the difficulty of launching a low-level DoS attack against WSNs.

The analysis of the threat faced from low-level DoS attacks and the analysis of the existing and proposed DoS defences are conducted on the home automation test-bed introduced in Chapter 3. Although the test-bed adopts the ZigBee WSN standard, the results are equally applicable to other WSNs. One of the reasons why the home automation test-bed is based on the ZigBee standard is because it is a relatively high data rate WSN standard with a higher level of resources compared to the alternative WSN standards. Consequently, although the low-level DoS threat is only evaluated against the ZigBee standard in this thesis, the lessons learned can be applied to the majority of other WSNs based on the IEEE 802.15.4 standard and those that have fewer resources than the ZigBee standard. Similarly, the experiments base the effectiveness of the simulation of existing DoS defence approaches on the D-WARD defence approach. However, from the literature review the D-WARD defence approach has been identified as one of the most effective approaches for detecting and filtering out suspected attack traffic. Consequently, the approach is representative of other DoS defence approaches that are reported to be less effective.

The experiments have shown that, as theorised, it is practically possible to launch a sufficiently large DoS attack that will permit a low-level of DoS attack

traffic to reach the intended victim and cause a serious disruption to communication between the entities on the WSN and remote users wishing to access the WSN. In the case of the experiments, ten trials were conducted involving a flooding DoS attack on a WSN based HAS in a star and partial mesh configuration, with only the existing D-WARD DoS defences in place. The experiment highlighted that in the star configuration, at the highest attack rate investigated of 256ppm, an average packet loss rate of 86.25% (a minimum of 84.38% and a maximum of 93.75%) was recorded. In the partial mesh configuration, the 256ppm attack rate resulted in an average packet loss rate of 91.25% (a minimum of 85.75% and a maximum of 94.75%).

Moreover, the experiments have shown that using the proposed defence approach alongside the existing defences, an attack can be effectively detected and appropriate resolution measures taken. In the case of the WSN based HAS in the star topology, the proposed defence approach has been shown to reduce the percentage packet loss on the WSN, during a flooding DoS attack, by a minimum of 84.70% for all of the 10 trials, with an average reduction of 91.13% and a maximum reduction of 95.6%. In the case of the WSN based HAS in the partial mesh topology, the proposed defence approach has been shown to reduce the percentage packet loss on the WSN, during a flooding DoS attack, by a minimum of 78.34% for all of the 10 trials, with an average reduction of 91.20% and a maximum reduction of 95.60%.

Additionally, the proposed approach has reduced the average connection latency experienced by remote users connecting to a WSN based HAS during an effective DoS attack against the gateway sensor node in all of the trials conducted. In an experiment with a 799 attacks per minute rate, the proposed approach resulted in a minimum reduction in connection latency of 56.11%, an average reduction of 56.71%, and a maximum reduction of 57.77%. In the experiment with a 2300 attacks per minute rate, the proposed approach resulted in a minimum reduction of connection latency of 90.14%, an average reduction of 90.90%, and a maximum reduction of 91.88%.

Chapter 8

Findings and Evaluations from Field-Trials

8.1 Background and Motivation

This chapter presents the key findings from the user evaluation of the research project. The user feedback extends the black box testing, integration testing, and the performance evaluation of the proposed DoS mitigation approaches presented earlier, alongside the respective DoS mitigation approaches in Chapters 5 – 7. This chapter presents the findings from a study to establish the validity of the home automation test-bed as an effective HAS. Furthermore, the results from a case study to evaluate the performance of the proposed DoS mitigation schemes to establish the practical applicability of the approaches is presented. Additionally, the first study to examine the potential human computer interaction challenges to arise from the adoption of home automation, the addition of remote connectivity to home automation, and different DoS mitigation approaches is presented.

8.2 Home Automation Test-Bed Validation

A twelve-day field trial was conducted, as part of a larger study into home automation, where the system was installed into the home of a potential user. As

part of the field trial, the users were given a questionnaire (See Appendix A) after the twelve-day trial period had ended to establish if the home automation test-bed functioned correctly and if in the opinion of the users the home automation test-bed represented a practical, viable implementation of a HAS. Due to the difficulty in obtaining participants for the field trial, the system was only trialled in the home of one potential user. To extend the study a separate focus group was held, where individuals were invited to attend a demonstration of the home automation test-bed and complete the same questionnaire as the field trial participants. From the analysis of the questionnaires, there was no discernable difference between the views of the field trial participants and those of the focus group participants. Consequently, the findings from the field trial and focus group studies are grouped together, as follows.

The study consisted of 12 participants. From which, 50% were homeowners and 50% lived in rented accommodation. The years the participants had resided at their current property ranged from 0-5 Years (58%) to more than 12 years (42%). There was a varied range of computer expertise amongst the participants, 42% had no or little experience operating computers, and 58% considered themselves advanced or expert users. Most of the users had little prior experience with advanced home automation technology; the most advanced systems commonly included in participant's homes included Smoke Alarms (67%), Central Heating System (75%), Burglar Alarms (58%), and Surveillance System (8%).

The home automation test-bed endeavours to incorporate existing technologies that users are familiar with, happy to use, and has the potential to lower systems cost. Consequently, the participants were asked which networking technologies were already available in their homes. The findings showed that Wi-Fi (IEEE 802.11b/g/n) was the most wide spread networking standard, available in 75% of participants homes. The Bluetooth standard was the second most widely adopted standard available in 58% of participants' homes. The only other networking standard identified to be available in 8% of participants' homes was Ethernet. This supports the incorporation of the Wi-Fi standard as part of the home automation test-bed, for use as the point of ingress between the HAS's, local network and the Internet.

Additionally, to verify the home automation test-beds focus on achieving a low cost approach, the participants were asked the maximum they would be willing to spend on a generic home automation infrastructure, excluding any high-end, consumer, network-enabled devices such as televisions. Most participants (58%) said less than £500, (92%) said less than £800, and only 8% stated they would be willing to pay more than £800. This indicates the low-cost concept adopted for the design of the home automation test-bed is in-line with the fiscal constraints of participants.

The participants were also asked how willing they were to purchase such a system as the home automation test-bed. The majority of participants (58%) said they would be likely to very likely to purchase such a system, 9% did not state an opinion and 33% said they were unlikely to very unlikely to purchase such a system.

It can be concluded, that the home automation test-bed's low-cost emphasis and integration with existing technologies, which are available in the vast majority of participant's homes, is in-line with the low price most participants are willing to pay for such systems. Moreover, the high acceptance of the home automation test-bed as a potential product that participants would strongly consider purchasing suggests the appropriateness of the test-bed for the evaluation of the security mechanisms proposed as part of the research.

8.3 Case Study Based System Evaluation

The evaluation of the proposed approach for securely communicating with WSN based HASs was based on a case study, where users were taken through a scenario. The evaluation was conducted in four stages. Firstly, the performance of the RHS-1 and RHS-2 communication approaches, introduced in Chapter 6, as a means for communicating with a WSN based HAS were evaluated. Secondly, the effectiveness of the hybrid communications approach, discussed in Chapter 6, for mitigating DoS attacks against a third party (RHS) was evaluated. Thirdly, the effectiveness of the hybrid communications approach, discussed in Chapter 7, for mitigating low-level DoS attacks targeted directly at the WSN based HAS was evaluated. Finally, the users perspectives of the integrated communication system as

an effective and secure solution for communicating with WSN based HASs were captured.

8.3.1 Scenario

The scenario consisted of the HAS test-bed and a mobile phone for remotely communicating with the HAS. Before the evaluation the participants were given a demonstration of the HAS to familiarise themselves with the system and introduced to the RHS-1 and RHS-2 communications approaches. The study consisted of ten participants. At the start of the study, the participants were asked to complete two demographic questions from a questionnaire (See Appendix B).

Once, the evaluation was started the HAS was run and participants were asked to control the system from a mobile phone. Additionally, the participants were informed that the system was currently using the RHS-2 method of communications. It was explained to the participants that the RHS-2 communication approach retrieves the IP address of the HAS from a third party and then directly communicates with the HAS for everyday communications tasks where security is not a critical requirement. The users were asked to keep viewing the status of devices and modifying devices connected to the HAS. The users were informed that a DoS attack would be launched against the HAS and that the system would automatically switch from the RHS-2 communications approach to the RHS-1 communications approach. The attack was conducted for a period of 5 minutes, after which the users were informed that the communication approach would switch back from the RHS-1 approach to the RHS-2 communications approach. The participants were asked to complete questions 3 to 8 of the questionnaire.

The exercise was repeated, however participants were informed that in the second instance the participants should assume that they are acting as a health professional accessing highly confidential and critical patient information. Consequently, the RHS-1 approach would be used as the securer communications approach for communications from the start. As before, the participants were informed when a DoS attack was started on the third party (RHS) and that the system would switch to using RHS-2 communications. The participants were asked to continue using the system until the attack had ended and the system returned to

using the RHS-1 communications approach. The participants were asked to complete questions 9 to 13 of the questionnaire.

In addition to the validation of the remote communications approaches the participants were asked to validate the effectiveness of the virtual home as a means for protecting the HAS from low-level DoS attacks. The participants were asked to use the HAS using a local controller to monitor and control devices. The participants were informed that the virtual home had been turned off and that the system was only protected using an existing DoS defence mechanism. The exercise was repeated with the virtual home turned on alongside existing DoS defence mechanisms. The participants were then asked to consider the different defence approaches and communication methods as part of a system for providing homeowners with everyday, high security, remote access communications and the potential for the system for protecting WSN based HASs from low-level DoS attacks. The Participants were then asked to complete the remainder of the questionnaire.

8.3.2 Case Study Findings

The case study consisted of 10 participants, of which 40% were male and 60% female. The participants ranged in age with 10% under 25 years, 50% aged 25-34 years, 10% aged 35-44 years, 20% aged 45 – 54 years and 10% aged 55 or over.

After the study had started and the HAS test-bed and RHS communication approaches (RHS-1 and RHS-2) had been discussed and demonstrated, the participants were asked how likely they were to adopt home automation technology in the future. The majority of participants agreed (20% Strongly Agree, and 40% Agree) that they felt they would adopt home automation technology in the future. Only 10% of participants felt they would not adopt any home automation technology in the future, with the remaining 30% adopting a neutral stance. Additionally, participants were asked if they would want remote access to their home automation devices, 70% agreed that they would want remote access (40% Strongly Agree, and 30% Agree). 10% of the participants stated they would not want remote access, and 20% took a neutral stance. This suggests that there is a significant demand for home automation technology. Moreover, that there is a

demand for people to be able to remotely access, monitor and control home automation devices.

After the participants had used the system for non-critical tasks using the RHS-2 approach and experienced an attack on the home gateway and the defence mechanism, responding to the attack. The participants were asked if the delay in accessing the HAS using the RHS-2 communication approach was acceptable. All of the participants agreed that the delay is acceptable (70% Strongly Agree, and 30% Agree). Moreover, the majority of participants agreed (40% Strongly Agree, and 40% agree) that they would be happy using the RHS-2 approach, which offers less security and increased performance for everyday non-critical communication tasks. Additionally, the participants were asked if they agreed that once the DoS attack started against the HAS, that the defence mechanism quickly recovered and that the delay in detecting the DoS attack and switching from the RHS-2 approach to the RHS-1 approach was acceptable. The majority of participants agreed (10% Strongly Agree, and 50% Agree) that the delay was acceptable. However, 30% of the participants disagreed that the delay was acceptable and 10% took a neutral stance. This suggests, the defence approach offers an acceptable level of service. Moreover, the delay experienced by the participants was purposely chosen to represent the maximum delay possible with the defence approach. Consequently, the delay a user will typically experience may be significantly less. Moreover, in a real situation the DoS attack and consequently the defence approach may operate during a period of inactivity, where users are not actively using the system, resulting in users experiencing no delay.

The participants were asked if they agreed that the defence approach dealt with their requests in an efficient and effective manner. The majority of the participants agreed (30% Strongly Agree, and 60% agree) that the system did. However, 10% of the participants did not agree that the system provided them with a satisfactory level of service. Although it should be noted that 10% represents the views of one of the participants. This suggests that the defence approach has real potential for further research and the development of a commercial defence approach based on the prototype defence approach.

The next stage of the study involved the users assuming that they are accessing highly personal information and critical service. The users were asked to use the RHS-1 approach and asked to evaluate this communication approach as before with the RHS-2 approach.

The participants were asked if they agreed that for accessing critical information and services they preferred to use the RHS-1 communications approach. All of the participants stated that they agreed (70% Strongly Agree, and 30% Agree). Furthermore when asked if they would be willing to use the RHS-2 approach in emergencies, 70% participants agreed (40% Strongly Agree, and 30% Agree) they would be willing to access critical services and information using the RHS-2 approach in emergencies, 20% Disagreed and 10% took a neutral stance. This suggests that although participants prefer using the security approach for critical tasks and for accessing personal information, they do not strongly object to using the RHS-2 approach infrequently during emergencies.

The majority of participants agreed (10% Strongly Agree, and 60% Agree) that the RHS-1 approach offers an acceptable delay for accessing the HAS. 20% took a neutral stance and 10% disagreed. This shows that the RHS-1 approach offers an acceptable level of delay for accessing HASs, where security is of greater importance than the speed of operations. However, the strength of this feeling was less than that expressed for the RHS-2 approach. However, this is not surprising as the RHS-1 communications approach is slower than the RHS-2 communications approach. However the time taken to detect and respond to a DoS attack is faster for the defence approach targeted at protecting the third party, than the previous defence approach for protecting the HAS. This resulted in all of the participants agreeing (40% Strongly Agree, and 60% Agree) that the delay in detecting and switching access approaches (RHS-1 to RHS-2) was acceptable. Moreover, 80% of the participants agreed that the defence approach for protecting the third party (RHS) from DoS attacks, dealt with all the users requests in an efficient and effective manner. This supports the potential for the third party defence approach for further research and for the development of the prototype defence approach into a commercial solution.

The effectiveness of the defence approaches for preventing DoS attacks reaching and affecting local communications on the WSN based HAS was investigated. The HAS test-bed was subjected to attack traffic without any defences. The participants were asked if they agreed that the HAS provided an acceptable level of performance. All of the participants disagreed (80% Strongly Disagree, 20% Disagree) with the statement. The exercise was repeated, however with a simulator representing existing DoS defence approaches removing the majority of the attack traffic, and only allowing a low-level of attack traffic to reach the HAS. All the participants (80% Strongly Disagree, 20% Disagree) disagreed that the HAS provides a satisfactory level of performance, whilst protected by existing defences. This is not surprising as even with the existing defences in place, the low-level attack traffic reaching the HAS is sufficient to degrade the systems performance, as discussed in Chapter 7. The exercise was repeated with the existing defences and the proposed defence approaches in place to prevent the low-level DoS attack traffic from reaching the HAS. All of the participants now agreed (70% Strongly Agree, and 30% Agree) that the HAS provided a satisfactory level of performance. This shows that the proposed defence approaches offer a valid defence against low-level DoS attack traffic.

The participants were then asked to comment on the general usability of the system as a whole, including the different defence mechanisms against DoS attacks and the underlying communication approaches. From the participants experience with the system most agreed that it is easy to use (10% Strongly Agree, and 70% Agree). The majority of the participants agreed (10% Strongly Agree, and 60% Agree) that they were comfortable using the different access approaches. Moreover, none of the participants disagreed that they were comfortable using the different communication approaches. Additionally, the participants were asked if they were happy to use a third party, as proposed in the RHS-1 and RHS-2 defence approaches. The majority of the participants agreed (20% Strongly Agree, and 50% Agree) that they were happy to use such a third party. This supports the conclusion that although users are not willing to use a third party, if it reduces their privacy, users are willing to use a third party if the communication approach provides sufficient protection against eavesdroppers at the third party. Furthermore, the majority of the participants agreed that they could effectively (20% Strongly Agree,

70% Agree, and 10% Disagree), efficiently (20% Strongly Agree, 60% Agree, 10% Neutral, and 10% Disagree), and happily use the proposed approaches for their HAS communication needs (20% Strongly Agree, 70% Agree, and 10% Disagree). This shows that the proposed approaches were well received by the participants and functioned correctly for the vast majority of participants.

8.4 Human Computer Interaction Challenges

During the first questionnaire (See Appendix A), directed at establishing the viability of the home automation test-bed, a section was included to identify human computer interaction issues arising from the provision of security for WSN based HASs. The study is the first to identify the issues that users adopting HASs have in regards to security.

The participants were asked to identify the features of a HAS that they find most desirable. The majority of participants (67%) ranked security of the HAS and their personal information as the number one consideration. The safety of the HAS was the second most desirable characteristic, with 50% of participants selecting it as their number two consideration. Likewise, energy saving was selected by 50% of the participant as the third most important feature. The features participates placed the least importance on were Multimedia and Tele-health system, being the participants fourth (42%) and fifth (50%) most important features of a HAS. This analysis shows that participants place a considerable importance on the level of security a system offers. Surprisingly, Tele-health systems ranked last in the features participants placed a greater importance on. The consistent reason given for this decision was that a Tele-health system would not benefit them directly until old age. Moreover, the participants aged 55 and over indicated they preferred going to see a doctor or other health care professional.

There are four primary security threats introduced by the adoption of a HAS. The participants were shown a list of these threats, with a description of each, and asked to select the threats they had previously heard about. From the participants responses 67% were aware that there was a risk of someone illegally accessing their HAS. 50% of participants were aware of the risk that a third party might monitor their communications between remote users and the HAS. 67% of participants were

aware that there was a potential risk to their personal information stored on the HAS. Moreover, 42% of the participants were concerned that they might not be able to access their HAS because an attacker may launch a DoS attack against their HAS. It should be noted that participants were not generally aware of the term DoS. However, the participants identified with media stories of attackers launching similar attacks against organisations.

The participants were asked to state which of these issues most concerned them. All of the participants (100%) stated that they were most worried about attackers gaining access to their HAS and controlling HAS devices. 58% of participants chose the privacy threat to information stored on the HAS as the second threat they were most concerned about and 58% of participants chose the threat to privacy of information passed between remote users and the HAS as the third issue they were most concerned about.

Additionally, the participants were asked if one of the previously discussed issues was to arise, how they would like the HAS to address the situation. Most of the participants (75%) stated they would like the HAS to address the problem and inform them of the problem and any action the system had taken to resolve the threat. Moreover, 25% of the participants stated they would like the system to inform them of the problem and provide them with a list of possible solutions from which they would instruct the system on how best to solve the problem. It should be noted that none of the participants wanted the system to resolve the threat without informing them or take no action.

This shows that there is a general awareness amongst participants of a wide range of security issues. Moreover, even though the participants don't have a full understanding of all the security issues associated with HASs, they place a great deal of importance on a HAS that provides sufficient security measures to address these issues. Additionally, participants want to maintain a certain degree of control over the security situations that arise. The participants do not simply want to hand over complete control to an entirely automated system for dealing with security, they want to be informed of threats as they occur, and in the case of 25% of participants, select the action the system takes to resolve any potential threats.

The participants were asked questions regarding how intrusive they felt a HAS might be, and how comfortable they would be having their home environment monitored by such a system. The consensus was that the participants would be comfortable (17% extremely comfortable, and 75% comfortable), with only 8% of the participants choosing a neutral viewpoint. The participants were then asked how comfortable they would feel if the information the HAS monitors is stored locally within the home environment. Generally, the participants were still comfortable (25% extremely comfortable, 58% comfortable and 17% neutral) with this situation. However, when asked how comfortable the participants would feel if the information was stored or accessible by a third party, the situation changed drastically. The consensus was that participants were not comfortable (25% extremely uncomfortable, 50% uncomfortable) having their information stored or accessible on a third party. Only 17% of users were comfortable with a third party having access to, or storing their personal information, with 8% taking a neutral stance. Moreover, when asked how concerned participants were about the threat to privacy from HASs, the majority indicated that they were concerned (17% extremely concerned, and 75% Concerned).

This analysis shows that although homeowners are happy with their personal information being monitored, transmitted, and stored locally, most participants do not sufficiently trust third parties to monitor, transmit, and store their personal information. Consequently, this finding supports the privacy aspects of the RHS communication approaches used as part of the DoS defence mechanisms, which although incorporate a third party, do not make the homeowners personal information available to anyone except the homeowners.

The participants were asked how comfortable they were handing control over to a HAS. The majority of the participants were uncomfortable (41%) with handing over control to a HAS, if they could not change settings the system made. 25% of the participants preferred to take a neutral stance, and 34% said they were comfortable handing over complete control to a HAS. If the HAS gives the homeowners greater control to change settings made by the HAS, all of the participants (100%) said they would be comfortable (33% extremely comfortable, and 67% comfortable) handing control over to a HAS. This indicates that users want

a system that makes autonomous decisions in regards to everyday activities, however gives ultimate control over decisions to users. This supports the applicability of the HAS test-bed design which automates devices, however offers users a diverse range of methods to manually adjust settings. This further supports the home automation test-bed as a valid means of evaluating the security enhancements to the remote control architecture and WSN based HASs, conducted as part of the research.

8.5 Conclusions

This chapter has focused on the user evaluation of the proposed defence system, including the defence mechanisms incorporating the RHS-1 and RHS-2 communication approaches. It can be concluded that there is a demand for home automation technology, and that users desire to be able to control their devices from remote locations, such as work or while on holiday. The study has shown that there is a general understanding of security issues that might arise from the adoption of such systems. Even in instances where this awareness of security issues does not exist, users show the greatest concern over security issues and desire systems that will provide them with a high level of security. In this endeavour, homeowners are willing to accept the need for a third party, as part of a defence system, to provide them with added protection against security issues. However, the research has shown that there are significant human computer interaction factors that have to be overcome for HAS and third-party based communications approaches to be successfully adopted, primarily concerned with the confidentiality of homeowners personal information. Moreover, the user evaluation has demonstrated the weakness of existing DoS defence mechanisms for protecting WSN based HASs and the effectiveness of low-level DoS attacks against WSNs. Additionally, the user evaluation has shown that the defence system, proposed for securely and remotely communicating with WSN based HASs, meets the user's needs. Moreover, the approach provides a system that offers a secure communication approach, more resistance to low-level DoS attacks for WSNs, whilst incorporating communications approaches that provides an increased level of privacy for homeowner's personal information and which users find easy to use.

Chapter 9

Conclusions and Future Work

9.1 Summary

The concept of a home is something that most people share in common. Consequently, home automation has the potential to improve the quality of life of people throughout society. However, home automation must be adopted in a way that provides homeowners with the maximum improvement in quality of life, without sacrificing their personal privacy or right to control their home environment as they desire. The recent trend in academia and industry to design HASs based on low-cost, resource limited WSNs further adds to the difficulty of providing sufficient security. Through the analysis of existing HASs, communication approaches, and security mechanisms several weaknesses have been identified in providing sufficient security, primarily associated with the remote access, monitoring and control of WSN based HASs. Through the design and implementation of a third-party based secure remote access approach for WSN based HASs, it has been demonstrated that it is possible to overcome such flaws. Although, the proposed approach has been tested and implemented on a resource limited WSN based HAS, the approach is in principle extendible to other WSN applications. It can be surmised that the research represents a practical approach for the design and implementation of a securer automated home environment.

9.2 Contributions and Future Work

This thesis has contributed in enhancing the security of WSN based HASs. The purpose of this thesis is to investigate the suitability of existing security approaches for protecting resource limited WSN based HASs and the associated remote access approaches from privacy and availability threats. Moreover, where appropriate to develop approaches for enhancing the privacy and availability of WSN based HASs and the associated remote access approaches. The main contributions and findings from the research are listed below:

1. **The design of a WSN based HAS test-bed for the practical evaluation of security approaches.** The thesis presents the design of a WSN based HAS, with the underlying infrastructure for security mechanisms to be added and practically evaluated. The majority of existing security mechanisms are theoretically evaluated or tested with simulators. The design of a HAS test-bed allows for the existing security approaches and proposed security approaches to be evaluated on a real HAS, adding to knowledge from a different perspective. Moreover, the test-bed allows for the creation of benchmarks from existing approaches (GHS and D-WARD) to contrast with the proposed approaches (RHS-1, RHS-2, and Hybrid). A summary of the quantitative analysis derived from the use of the WSN based HAS test-bed are presented in the following contributions.

2. **A comprehensive analysis of remote access approaches and the related privacy and availability threats for WSN based HASs.** This thesis presents the first study to summarise the existing methods for remotely accessing, monitoring, and controlling HASs. Namely, the Direct and GHS communications approach. The approaches have been qualitatively evaluated to highlight the direct access approach is not suitable for monitoring and controlling WSN based HASs, due to the dynamic nature of the IP addresses in the UK, where the IP address of a HAS cannot be known before a direct connection attempt. Moreover, the approaches have been quantitatively evaluated to show that the direct access approach is the fastest of the existing remote access approaches

analysed to login, share secure parameters and send three consecutive commands, taking on average 2661ms (a minimum of 2604ms and a maximum of 2793ms). For the same experiments, the GHS approach is shown to be a minimum of 39.23% slower, on average 45.81% slower, and a maximum of 46.60% slower.

3. **Identification and resolution of a vulnerability, in communications privacy for third party mediated remote communications.** A vulnerability in the communications privacy of remote users communicating with HASs using existing third party mediated communications approaches has been identified, at the third party. The vulnerability allows users at the third party to view homeowner's confidential information, when it is decrypted at the third party for rerouting. Consequently, a secure tunnelling approach for protecting the communications privacy of remote users communicating with WSN based HASs (called the RHS-1 approach) has been designed and implemented. The dual tunnelling method adopted in the RHS-1 approach removes 100% of the confidential information that is visible using the current GHS communications approach.

4. **Design of a hybrid communications approach for mitigating DoS attacks against a third party during third party based communications.** During an effective DoS attack against a third party, it has been shown that effective communications between a remote user and a WSN based HAS can be disrupted or completely blocked. A hybrid communications approach is designed and implemented, that incorporates the RHS-1 communication approach for critical communications. The RHS-1 approach has been quantitatively analysed in terms of performance and shown to be the slowest approach analysed in the research being a minimum of 86.85% slower, on average 92.78% (5130ms) slower, and a maximum of 95.60% slower than the direct access approach. The hybrid communications approach uses a direct approach to connect to the HAS for non-critical communications (called the RHS-2 approach), using the third party as a DNS to retrieve the IP

address of the respective HAS only when an old IP address has expired. The RHS-2 approach has been quantitatively analysed in terms of performance and shown to be a minimum of 19,8% slower, on average 20.59% slower, and a maximum of 20.80% slower than the direct access approach. Moreover, the hybrid communications approach has been quantitatively analysed in terms of the improvement of DoS resistance compared to the benchmark GHS approach. The results shows that compared to the GHS approach the proposed hybrid approach decreases the time the HAS services are unavailable by a minimum of 58.28%, on average by 59.85%, and a maximum of 61.45%.

5. **Identification of low-level DoS attack and the design of a hybrid approach for mitigating low-level DoS attacks targeted at WSN based HASs.** This thesis presents an analysis and experimental evaluation of a generic model representing existing DoS defences. The model represents the most effective DoS mitigation tool identified from the domain analysis D-WARD. The evaluation shows that this approach and the vast majority of existing approaches, that are less effective than the defence modelled, are ineffective for protecting resource limited WSN based HASs. The evaluation highlighted that a flooding DoS attack directly targeting a WSN based HAS in a star configuration, at a 256ppm attack rate, results in a sufficient amount of attack data penetrating the existing D-WARD DoS defences to result in an average packet loss rate of 86.25% (a minimum of 84.38% and a maximum of 93.75%). In the partial mesh configuration, the 256ppm attack rate results in an average packet loss rate of 91.25% (a minimum of 85.75% and a maximum of 94.75%). Moreover, a flooding DoS attack targeting the home gateway at 1090 attacks per minute, results in a minimum connection latency of 7130ms, an average latency of 7431ms and a maximum latency of 7942ms. A defence called the “virtual home” is implemented at the edge of the WSN, alongside existing defences, to filter all incoming traffic, using a cryptographic approach to remove all attack traffic, preventing it from reaching and disrupting the WSN.

The virtual home has been experimentally shown to reduce the percentage packet loss on the WSN during an effective DoS attack.
In the case of the WSN based HAS in the star topology, the proposed defence approach has been shown to reduce the percentage packet loss on the WSN, during a flooding DoS attack, by a minimum of 84.70%, with an average reduction of 91.13% and a maximum reduction of 95.6%. In the case of the WSN based HAS in the partial mesh topology, the proposed defence approach has been shown to reduce the percentage packet loss by a minimum of 78.34%, with an average reduction of 91.20% and a maximum reduction of 95.60%.

Additionally, the proposed approach has reduced the average connection latency experienced by remote users connecting to a WSN based HAS during an effective DoS attack against the gateway sensor node in all of the trials conducted. In an experiment with a 799 attacks per minute rate, the proposed approach resulted in a minimum reduction in connection latency of 56.11%, an average reduction of 56.71%, and a maximum reduction of 57.77%. In the experiment with a 2300 attacks per minute rate, the proposed approach resulted in a minimum reduction of connection latency of 90.14%, an average reduction of 90.90%, and a maximum reduction of 91.88%.

Finally, this thesis has achieved all of the proposed objectives described in Chapter 1. Future work in enhancing the security of WSN based HASs should focus on enhancing the detection accuracy, and reducing the time delay in detecting DoS threats. Moreover, the speed of the response mechanisms once an attack is detected can be optimised. Additionally, we hope that the research presented in this thesis helps to stimulate research into secure and reliable remote access approaches for WSN based HASs. Especially, relating to the threats WSNs face from connected resource rich networks, such as the Internet.

References

[1] Akkaya, K. & Younis, M., “A Survey on routing protocols for wireless sensor networks”, *Ad Hoc Networks*, Vol. 3, No. 3, pp. 325-349, 2005.

[2] Akyildiz, I.F., Su, W., Sankarasubramaniam, Y. & Cyirci, E.,"A Survey on Sensor Networks", *IEEE Communications Magazine,* Vol. 40, No. 8, pp. 102-114, 2002.

[3] Aschenbernner, J.R.,"Open Systems Interconnection", *IBM System Journal,* Vol. 25, No. 3/4, pp. 369-379, 1986.

[4] Avison, D.E. & Fitzgerald, G., Information Systems Development:

Methodologies, Techniques and Tools, 3rd edn, McGraw Hill, 2003.

[5] Baker, C.R., Armijo, K., Belka, S., Benhabib, M., Bhargava, V., Burkhart, N., Der Minassians, A., Dervisoglu, G., Gutnik, L., Haick, M.B., Ho, C., Koplow, M., Mangold, J., Robinson, S., Rosa, M., Schwartz, M., Sims, C., Stoffregen, H., Waterbury, A., Leland, E.S., Pering, T. & Wright, P.K., "Wireless Sensor Networks for Home Health Care", *Advanced Information Networking and Applications Workshops*, pp. 832, 2007.

[6] Baker, F. & Savola, P., "Ingress Filtering for Multihomed Networks, Network Working Group"*, http://www.ietf.org/rfc/rfc3704.txt*, 2004.

[7] Barontib, P., Pillaia, P., Chooka, V.W.C., Chessab, S., Gottab, A. & Hua, Y.F.,"Wireless sensor networks: A survey on the state of the art and the 802.15.4 and ZigBee standards", *Computer Communications,* Vol. 30, No. 7, pp. 1655-1695, 2007.

[8] Bausell, R.B., "Practical Guide to Conducting Empirical Research", *Longman Higher Education*, 1986.

[9] BBC, "New Cyber Attacks Hit S Korea", *http://news.bbc.co.uk/1/hi/world/asia-pacific/8142282.stm*, 2009.

[10] Bergstrom, P., Driscoll, K. & Kimball, J., "Making home automation communications secure", *Computer,* Vol. 34, No. 10, pp. 50-56, 2001.

[11] Bouncycastle, "The Legion of the Bouncy Castle", http://www.bouncycastle.org, 2009.

[12] Bolzani, C.A.M., Montagnoli, C. & Netto, M.L., "Domotics Over IEEE 802.15.4 - A Spread Spectrum Home Automation Application", *Ninth International Spread Spectrum Techniques and Applications Conference*, pp. 396-402, 2006.

[13] British Standards Institution, "What is a standard", *http://www.bsi-global.com/*, 2009.

[14] Bromley, K., Perry, M. & Webb, G., "Trends in smart home systems, connectivity and services", Building Research Establishment, 2003.

[15] Burstein, F., "System Development in Information Systems Research", *Research Methods for Students, Academics and Professionals: Information Management and Systems*, 2nd edn, Centre for Information Studies, Charles Sturt University, Wagga, pp. 147-158, 2002.

[16] Burton, E., Sir., *"Report into the Loss of MOD Personal Data"*, Ministry of Defence, 2008.

[17] Chang, R.K.C.,"Defending against flooding-based distributed denial-of-service attacks: a tutorial", *IEEE Communications Magazine,* Vol. 40, No. 10, pp. 42-51, 2002.

[18] Cheung, S.,"Denial of Service against the Domain Name System", *IEEE Security and Privacy archive,* Vol. 4, No. 1, pp. 40-45, 2006.

[19] Chiba, T., Katoh, T., Bista, B.B. & Takata, T., "DoS packet filter using DNS information", *20th International Conference on Advanced Information Networking and Applications*, pp. 6-11, 2006.

[20] Collotta, M., Nicolosi, G., Toscano, E. & Mirabella, O., "A ZigBee-based network for home heating control", *34th Annual Conference of IEEE Industrial Electronics Society,* 2009.

[21] Corcoran, P.M., Desbonnet, J. & Lusted, K., "CEBus Network Access via the World-Wide-Web", *International Conference on Consumer Electronics*, pp. 236-239, 1996.

[22] Cotroneo, D., Peluso, L., Romano, S.P. & Ventre, G., "An active security protocol against DoS attacks", *Proceedings of the Seventh International Symposium on Computers and Communications*, pp. 496-501, 2002.

[23] Craig, W., *"Zigbee:* Wireless Control That Simply Works*"*,

http://www.zigbeeresourceguide.com/images/ZigBee_RG_2008.pdf, 2005.

[24] Crosby, G.V., Pissinou, N. & Gadze, J., "A Framework for Trust-based Cluster Head Election in Wireless Sensor Networks", *Second IEEE Workshop on Dependability and Security in Sensor Networks and Systems*, pp. 13-18, 2006.

[25] CS3 inc, The Reverse Firewall: Defeating DDoS Attacks Emanating from a Local Area Network*, http://www.cs3-inc.com/rfw.html*, 2009.

[26] CS3 inc, "MANAnet: Infrastructure-level DDoS Defense"*, http://www.cs3-inc.com/mananet.html*, 2008.

[27] Das, V.V., "Honeypot Scheme for Distributed Denial-of-Service", *International Conference on Advanced Computer Control*, pp. 497-502, 2009.

[28] Deng, J., Han, R. & Mishra, S., "Defending against path-based DoS attacks in wireless sensor networks", *Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks*, New York, USA, pp. 89-94, 2005.

[29] Deng, J., Han, R. & Mishra, S., "Intrusion tolerance and anti-traffic analysis strategies for wireless sensor networks", *International Conference on Dependable Systems and Networks*, pp. 637-642, 2004.

[30] Digi, www.digi.com, 2009.

[31] Duncan, R. & Shabot, M.,"Secure remote access to a clinical data repository using a wireless personal digital assistant (PDA)", *Journal of the American Medical Informatics Association,* pp. 210-214, 2000.

[32] Ergen, S.C.*,"ZigBee/IEEE 802.15.4 Summary",* 2004.

[33] Garber, L.,"Denial of Service Attacks Rip the Internet", IEEE *Computer,* Vol. 33, No. 4, pp. 12-17, 2000.

[34] Gauger, M., Minder, D., Marrón, P.J., Wacker, A. & Lachenmann, A., "Prototyping sensor-actuator networks for home automation", *Proceedings of the workshop on Real-world wireless sensor networks*, New York, USA, pp. 56-61, 2008.

[35] Gill, K., Yao, F. & Yang, S.H., "The Design and Implementation of a Flexible Home Gateway Architecture", *The 13th International Conference on Automation and Computing*, Staffordshire, pp. 128-133, 2007.

[36] Gill, K. & Yang, S.H.,"Secure Remote Access for Home Automation Systems", *Measurement + Control,* 2008a.

[37] Gill, K., Yao, F. & Yang, S.H., "Transparent Heterogeneous Networks for Remote Control of Home Environments", *IEEE International Conference on Network Sensing and Control*, Sanya, China, pp. 1419-1424, 2008b.

[38] Gill, K., Yang, S.H., Yao, F. & Lu, X.,"A ZigBee Based Home Automation System", *IEEE Transactions on Consumer Electronics,* Vol. 55, No. 2, pp. 422-430, 2009a.

[39] Gill, K. & Yang, S.H., "A Scheme for Preventing Denial of Service Attacks on Wireless Sensor Networks", *The Proceedings of the 35th Annual Conference of the IEEE Industrial Electronics Society*, Porto, 2009b.

[40] Grottke, M., Sun, H., Fricks, R.M. & Trivedi, K.S., "Ten Fallacies of Availability and Reliability Analysis", *5th International Service Availability Symposium*, New York, USA, pp. 187, 2008.

[41] Hasan, H., "Information Systems Development as a Research Method", Australasian Journal of Information Systems, Vol. 11, No. 1, pp. 4-13, 2004.

[42] Hawizy, L., "A Semiotic Approach to Ad-Hoc Networked Environments ", Loughborough University, http://hdl.handle.net/2134/3146, 2007.

[43] Horrocks, P., "Stop the Blocking Now", BBC*, http://www.bbc.co.uk/blogs/theeditors/2009/06/stop_the_blocking_now.html*, 2009.

[44] Hu, Y., Yin, H., Lin, C., Jiang, X., Ouyang, Y., & Li, C., "CSGW-RAS: A novel secure solution for remote access based on SSL", *International Symposium on Intelligent Signal Processing and Communication Systems*, pp. 798-803, 2007.

[45] Hwang, M. & Li, L.,"A new remote user authentication scheme using smart cards", *IEEE Transactions on Consumer Electronics,* Vol. 46, No. 1, pp. 28-30, 2000.

[46] Hyun, S., Ning, P., Liu, A. & Du, W., "Seluge: Secure and DoS-Resistant Code Dissemination in Wireless Sensor Networks", *International Conference on Information Processing in Sensor Networks*, pp. 445-450, 2008.

[47] ICO*, "*Virgin Media Limited found in breach of data protection", *Information Commissioners Office*, 2008.

[48] indeedNET, Integration and demonstartion of energy efficient dwelling networks, Loughborough University*, www.indeednet.org*, 2007.

[49] Jennic, www.jennic.com, 2009.

[50] Jin, J., Wang, Y., Zhao, K. & Hu, J., "Development of Remote-Controlled Home Automation System with Wireless Sensor Network", *Fifth IEEE International Symposium on Embedded Computing*, pp. 169-174,2008.

[51] Kara, A., "Private-to-Private communications over the internet", *IEEE Computer,* Vol. 37, No. 5, pp. 53-59, 2004.

[52] Kara, A.*,* "Secure remote access from office to home"*, IEEE Communications Magazine,* Vol. 39, No. 10, pp. 68-72, 2001.

[53] Keromytis, A.D., Misra, V. & Rubenstein, D., "SOS: secure overlay services", *Proceedings of the 2002 conference on Applications, technologies, architectures, and protocols for computer communications*, New York, USA, pp. 61-66, 2002.

[54] Khurram, K.M. & Jiashu, Z.,"Improving the security of 'a flexible biometrics remote user authentication scheme'", *Computer standards & interfaces.,* Vol. 29, No. 1, pp. 82-85, 2007.

[55] Kihong, P. & Heejo, L., "On the Effectiveness of Route-Based Packet Filtering for Distributed DoS Attack Prevention in Power-Law Internets", ACM SIGCOMM Computer Communications Review, Vol. 31, No. 4, pp. 15-26, 2001.

[56] Ku, W. & Chen, S.,"Weaknesses and improvements of an efficient password based remote user authentication scheme using smart cards", *IEEE Transactions on Consumer Electronics,* Vol. 50, No. 1, pp. 204-207, 2004.

[57] Kumar, S., Valdez, R., Gomez, O. & Bose, S., "Survivability Evaluation of Wireless Sensor Network under DDoS Attack", *International Conference on Networking, International Conference on Systems and International*

Conference on Mobile Communications and Learning Technologies, pp. 82-89, 2006.

[58] Kuorilehto, M., Suhonen, J., Kohvakka, M., Hannikainen, M., & Hamalainen, T.D., "Experimenting TCP/IP for Low-Power Wireless Sensor Networks", *IEEE 17th International Symposium on Personal, Indoor and Mobile Radio Communications*, pp. 1-6, 2006.

[59] Law, Y.W., Hoesel, L.V., Doumen, J., Hartel, P. & Havinga, P., "Energy-efficient link-layer jamming attacks against wireless sensor network MAC protocols", *Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks*, USA, pp. 76-81, 2005.

[60] Lewis, F.L.,"Smart Environments: Technology, Protocol and Applications, "*Wireless Sensor Networks*, eds. D.J. Cook & S.K. Das, 1st edn, John Wiley, New York, USA, pp. 13-46, 2004.

[61] Li, B. & Batten, L., "Using mobile agents to detect node compromise in path-based DoS attacks on wireless sensor networks", *Proceedings of the International Conference on Wireless Communications Networking and Mobile Computing*, pp. 2507-2512, 2007.

[62] Linx, P., My WiFi Technology, Intel, *www.intel.com/network/connectivity/products/wireless/mywifi.htm*, 2009.

[63] Liu, D. & Ning, P., "Efficient Distribution of Key Chain Commitments for Broadcast Authentication in Distributed Sensor Networks", *10th Annual Network and Distributed System Security Symposium*, San Diego, California, USA, pp. 102-115, 2003.

[64] Mahimkar, A., Dange, J., Shmatikov, V., Vin, H. & Zhang, Y., "dFence: Transparent Network-based Denial of Service Mitigation", , 4th USENIX Symposium on Networked Systems Design & Implementation, pp. 327-332, 2007.

[65] Malan, G.R., Watson, D., Jahanian, F. & Howell, P., "Transport and application protocol scrubbing", *INFOCOM Nineteenth Annual Joint*

Conference of the IEEE Computer and Communications Societies., Tel Aviv, pp. 1381-1386, 2002.

[66] Microsystems, S., IP Denial-of-Service Attacks, CERT, *http://www.cert.org/advisories/CA-1997-28.html*, 1998.

[67] Mirkovic, J., *D-WARD Source-End Defense Against Distributed Denial of Service Atacks*, University of California, 2003.

[68] Mirkovic, J. & Reiher, P.,"A taxonomy of DDoS attack and DDoS defense mechanisms", *ACM SIGCOMM Computer Communication Review,* Vol. 34, No. 2, pp. 39-53, 2004.

[69] National Statistics, Internet Access, National Statistics, *http://www.statistics.gov.uk/cci/nugget.asp?id=8*, 2008.

[70] Paxson, S., "An analysis of using reflectors for distributed denial-of-service attacks", *ACM SIGCOMM Computer Communication Review,* Vol. 31, No. 3, pp. 38-47, 2001.

[71] Perrig, A., Szewczyk, R., Tygar, J.D., Wen, V. & Culler, D.E.,"SPINS: security protocols for sensor networks", *Wireless Networks,* Vol. 8, No. 5, pp. 521-534, 2002.

[72] Perrig, A., Szewczyk, R., & Wagner, D., "Security in Wireless Sensor Networks", *Communications of the ACM*, Vol. 47, No. 6, pp 53-57, 2004.

[73] Polastre, J., Hill, J. & Culler, D., "Versatile low power media access for wireless sensor networks", *Proceedings of the 2nd international conference on Embedded networked sensor systems*, New York, USA, pp. 95-101, 2004.

[74] Poynter, K., *Review of information security at HM Revenue and Customs*, HM Treasury, 2008.

[75] Rahman, A. & Gburzynski, P., "Hidden Problems with the Hidden Node Problem", *Proceedings of the 23rd Biennial Symposium on Communications*, pp. 270-274, 2006.

[76] Ratul, M., Steven, M.B., Sally, F., John, I., Vern, P. & Shenker, S., "Controlling High Bandwidth Aggregates in the Network", *ACM SIGCOMM Computer Communication Review*, pp. 62-72, 2002.

[77] Raymond, D.R., Marchany, R.C., Brownfield, M.I. & Midkiff, S.F.,"Effects of Denial-of-Sleep Attacks on Wireless Sensor Network MAC Protocols", *IEEE Transactions on Vehicular Technology,* Vol. 58, No. 1, pp. 367-380, 2009.

[78] Raymond, D.R. & Midkiff, S.F.,"Denial-of-Service in Wireless Sensor Networks: Attacks and Defenses", *IEEE Pervasive Computing,* Vol. 7, No. 1, pp. 74-81, 2008.

[79] Reinisch, C., Kastner, W., Neugschwandtner, G. & Granzer, W., "Wireless Technologies in Home and Building Automation", *5th IEEE International Conference on Industrial Informatics*, pp. 93-98, 2007.

[80] Salonidis, T., Bhagwat, P., Tassiulas, L., Tassiulas, R. & LaMaire, R.,"Distributed Topology Construction of Bluetooth Wireless Personal Area Networks", *IEEE Journal on Communications,* Vol. 23, No. 3, pp. 633-643, 2005.

[81] Santos, R.A., Edwards, A., Alvarez, O., Gonzalez, A. & Verduzco, A., "A Geographic Routing Algorithm for Wireless Sensor Networks", *IEEE Electronics Robotics and Automotive Mechanics Conference*, pp. 64-69, 2006.

[82] Schuba, C.L., Krsul, I.V., Kuhn, M.G. & Spafford, E.H., "Analysis of a Denial of Service Attack on TCP", *Proceedings of the 1997 IEEE Symposium on Security and Privacy*, Washington, DC, USA, pp. 208-303,1997.

[83] Shen, J., Lin, C. & Hwang, M.,"A modified remote user authentication scheme using smart cards", *IEEE Transactions on Consumer Electronics,* Vol. 49, No. 2, pp. 414-416, 2003.

[84] Shuaib, K., Boulmalf, M., Sallabi, F. & Lakas, A., "Co-existence of Zigbee and WLAN - a performance study", *2006 IFIP International Conference on, Wireless and Optical communications*, pp. 5-11, 2006.

[85] Sriskanthan, N., Tan, F. & Karande, A.,"Bluetooth based home automation system", *Microprocessors and Microsystems,* Vol. 26, No. 6, pp. 281-289, 2002.

[86] Stajano, F. & Anderson, R.J., "The Resurrecting Duckling: Security Issues for Ad-hoc Wireless Networks", *Proceedings of the 7th International Workshop on Security Protocols*, pp. 172-177, 1999.

[87] Stallings, W*., Cryptography and Network Security Principles and Practices,* 3rd edn, Prentice Hall, 2002.

[88] Sun, M., Liu, Q. & Jiang, M., "An implementation of remote lighting control system based on Zigbee technology and SoC solution", *IEEE International Conference on Audio, Language and Image Processing*, pp. 629-632, 2008.

[89] Sun, H.,"An efficient remote use authentication scheme using smart cards", *IEEE Transactions on Consumer Electronics,* Vol. 46, No. 4, pp. 958-961, 2000.

[90] Tanenbaum, A.S*., Computer Networks,* 4th edn, Prentice Hall 2003.

[91] Thomas, R., Mark, B., Johnson, T. & Croall, J., "NetBouncer: client-legitimacy-based high-performance DDoS filtering", *Proceedings of the Information Survivability Conference and Exposition*, pp. 14-19, 2003.

[92] Thomer, M.G. & Massimiliano, P., "MULTOPS: a data-structure for bandwidth attack detection", *Proceedings of 10th Usenix Security Symposium*, pp. 23-29, 2001.

[93] Touch, J.D., Finn, G.G., Wang, Y. & Eggert, L., "DynaBone: dynamic defense using multi-layer Internet overlays", *Proceedings of DARPA Information Survivability Conference and Exposition*, pp. 271-276, 2003.

[94] Varchola, M. & Drutarovsky, M.,"Zigbee Based Home Automation Wireless Sensor Network", *Acta Electrotechnica et Informatica,* Vol. 7, No. 4, 2007.

[95] Virone, G., Wood, A., Selavo, L., Cao, Q., Fang, L., Doan, T., He, Z., Stoleru, R., Lin, S. & Stankovic, J.A., "An Assisted Living Oriented Information

System Based on a Residential Wireless Sensor Network", *1st Transdisciplinary Distributed Diagnosis and Home Healthcare Conference*, pp. 95-99, 2006.

[96] Wang, H., Zhang, D. & Shin, K.G., "Detecting SYN flooding attacks", *Proceedings of the Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies*, USA, pp. 1530-1526, 2002.

[97] Weiler, N., "Honeypots for distributed denial-of-service attacks", *Proceedings of the Eleventh IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises*, Washington, DC, USA, pp. 109-114, 2002.

[98] Wood, A.D. & Stankovic, J.A.,"A Taxonomy for Denial-of-Service Attacks in Wireless Sensor Networks"*Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems*, eds. M. Ilyas & I. Mahgoub, 1st edn, CRC Press, , 2004.

[99] Wood, A.D. & Stankovic, J.A.,"Denial of service in sensor networks", *IEEE Computer,* Vol. 35, No. 10, pp. 54-62, 2002.

[100] Wu, J. & Qin, H., "The design of wireless intelligent home system base on ZigBee", *11th IEEE International Conference on Communication Technology*, pp. 73-78, 2008.

[101] Xiang, Y. & Zhou, W.,"Protecting web applications from DDoS attacks by an active distributed defense system", *International Journal of Web Information Systems,* Vol. 2, No. 1, pp. 37-44, 2006.

[102] Xu, W., Trappe, W., Zhang, Y. & Wood, T., "The feasibility of launching and detecting jamming attacks in wireless networks", *International Symposium on Mobile Ad Hoc Networking & Computing archive*, New York, pp. 46-57, 2005.

[103] Yang, M., Chau, D., Zeng, K., Chang, X., Cheng, F. & Wang, Q., "Intelligence and Security Informatics Techniques and Applications", Springer, 2008.

[104] Yao, F., Gill, K. & Yang, S., "A ZigBee Based Low Cost Automation System", *The 13th Annual Conference of Chinese Automation and Computing Society,* United Kingdom, pp. 258 - 263, 2007.

[105] ZigBee Alliance, ZigBee Specification 2007, ZigBee Alliance*,* *http://www.zigbee.org*, 2007.

Appendix A: Home Automation: Questionnaire

Dear Respondent,

Please complete the questionnaire as honestly and descriptively as possible. The answers you provide will be vital in the successful development of home automation technology that meets users' needs. Thank you in advance for your time and effort.

Please answer ***all*** questions by ticking the appropriate box(s) unless otherwise stated.

Section 1: Personal Information

1. Gender

   ☐ Male ☐ Female

2. Age group

   ☐ Under 25 ☐ 35 – 44 ☐ 55 and over

   ☐ 25 – 34 ☐ 45 – 54

3. Is the property you reside in owner occupied or rented?

   ☐ Owner Occupied ☐ Rented

4. How many years have you been residing in your current home?

   ☐ 0 – 2 ☐ 6 – 8 ☐ 12+

   ☐ 3 – 5 ☐ 9 – 11

5. How would you rate your level of computer experience?

   ☐ No experience

   ☐ Novice

   ☐ Intermediate

   ☐ Advanced

   ☐ Expert

Section 2: Home Automation

6. Which of the following ***automation systems*** are installed in your home?

☐ Fire Alarm ☐ Central Heating ☐ Multimedia

☐ Burglar Alarm ☐ Health Care ☐ Surveillance

☐ Other ☐ None

If 'Other', please specify below:

.....

.....

.....

7. Which of the following ***networks*** are available in your home?

☐ Wi-Fi ☐ X10 ☐ Bluetooth

☐ ZigBee ☐ Other ☐ None

If 'Other', please specify below:

.....

.....

.....

8. During the home automation trial Period did any of the devices have to be restarted?

☐ Yes ☐ No

If 'Yes', please clarify below, including approximately how many times devices were restarted:

.....

.....

.....

9. During the trial period did any of the home automation devices not function correctly?

☐ Yes ☐ No

If 'Yes', please clarify below:

.....

.....

.....

10. During the trial period did any of the home automation devices require a battery change?

☐ Yes ☐ No

If 'Yes', please state the device and approximate day of the respective battery change:

.....
.....
.....

11. Do you feel that the automatic radiator valve helped control the temperature in your home more accurately than your existing radiator valve?

☐ Strongly Agree

☐ Agree

☐ Neutral

☐ Disagree

☐ Strongly Disagree

Please clarify below:

.....
.....
.....

12. Do you feel that the radiator valve would help you save energy by providing greater control over heating?

☐ Strongly Agree

☐ Agree

☐ Neutral

☐ Disagree

☐ Strongly Disagree

Please clarify below:

.....
.....
.....

13. Do you feel the information provided by the power meter helped you better understand how energy is used within your home?

☐ Strongly Agree

☐ Agree

☐ Neutral

☐ Disagree

☐ Strongly Disagree

Please clarify below:

.....
.....
.....

14. Do you feel that the information provided by the power meter would help you save energy?

☐ Strongly Agree

☐ Agree

☐ Neutral

☐ Disagree

☐ Strongly Disagree

Please clarify below:

.....
.....

15. Do you feel the delay in using the local controller to access devices is acceptable?

☐ Strongly Agree

☐ Agree

☐ Neutral

☐ Disagree

☐ Strongly Disagree

Please clarify below:

.....
.....
.....

16. Do you feel the delay in using the remote controller to access devices is acceptable?

☐ Strongly Agree

☐ Agree

☐ Neutral

☐ Disagree

☐ Strongly Disagree

Please clarify below:

.....

.....

17. Please rank the following home automation features from 1 (most attractive) to 5 (least attractive). *(Please see below for definition of phrases)*

☐ Security ☐ Multimedia ☐ Safety

☐ Tele-Health ☐ Energy saving

Please clarify:

.....

.....

.....

Security: *Protects the home from hackers controlling home automation devices and keeps home occupiers private information safe.*

Safety: *Protects the home occupiers by preventing dangerous events from happening.*

Tele-Health: *Monitors the occupier's health and may sound an alarm if the occupier's health diminishes.*

Multimedia: *Streams multimedia across the home to different rooms, this may include music or video.*

Energy Saving: *Monitors and aims to reduce the energy used in the home.*

18. In terms of an energy saving home automations system, what is the ***maximum number of years*** you would find acceptable to get a full return on your investment?

19. In terms of an energy saving home automation systems, what is the ***minimum percentage*** reduction in the total annual energy used by your home that you would find acceptable?

20 Based on the trial and your understanding of home automation how likely are you to consider investing in such a system in the future?

☐ Very Likely ☐ Likely ☐ Neutral ☐ Unlikely ☐ Very Unlikely

21. How much would you feel comfortable paying for a home automation system?

☐ £0 - £199
☐ £200 - £399
☐ £400 - £599
☐ £600 - £799
☐ £800+

Section 3: Home Automation Security

22. Please select, if any, the ***security*** issues you are aware of,

☐ Unauthorised access to the home automation system.

☐ Monitoring of communications between a remote device such as a mobile phone and the home automation system.

☐ Privacy threats to the personal information stored by the home automation system.

☐ Other

If 'Other', please specify below:

.....
.....
.....

23. Please number the importance you place on the following ***security*** issues from 1 (most important) to 3 (least important).

☐ Unauthorised access to the home automation system.

☐ Monitoring of communications between a remote device such as a mobile phone and the home automation system.

☐ Privacy threats to the personal information stored by the home automation system.

24. If a ***security*** situation such as "an unauthorised user gaining access to the system" was to arise, what would you like the home automation system to do? ***(Please select one answer only)***

☐ Try and resolve the situation and not inform you.

☐ Try and resolve the situation then inform you, allowing you to take further action if desired.

☐ Inform you of the situation and provide you with a list of possible solutions allowing you to choose the course of action to take.

☐ Inform you of the situation and take no action.

☐ Take no action.

25. Which statement below best completes the sentence?

A system that resolves the security issues highlighted would _____ to purchase a home automation system.

☐ Not encourage me

☐ Encourage me a little

☐ Encourage me

☐ Encourage me quite a bit

☐ Encourage me a great deal

Section 4: The Ethical Concerns of Home Automation

26. How comfortable do you feel about having the usage of your home appliances monitored by the home automation system?

- ☐ Extremely comfortable
- ☐ Comfortable
- ☐ Neutral
- ☐ Uncomfortable
- ☐ Extremely Uncomfortable

27. How comfortable do you feel about storing the information, regarding the usage of your home appliances, on ***your home automation system***?

- ☐ Extremely comfortable
- ☐ Comfortable
- ☐ Neutral
- ☐ Uncomfortable
- ☐ Extremely Uncomfortable

28. How comfortable do you feel about storing the information, regarding the usage of your home appliances, on ***a company database, outside of the home automation system***?

- ☐ Extremely comfortable
- ☐ Comfortable
- ☐ Neutral
- ☐ Uncomfortable
- ☐ Extremely Uncomfortable

29. How concerned are you regarding potential privacy risks associated with home automation systems? (i.e. a third party gaining access to personal information stored on the home automation system)

- ☐ Extremely Concerned
- ☐ Concerned
- ☐ Neutral
- ☐ Unconcerned
- ☐ Extremely Unconcerned

30. How comfortable are you in handing over control for certain home activities to a home automation system?

- ☐ Extremely comfortable
- ☐ Comfortable
- ☐ Neutral
- ☐ Uncomfortable
- ☐ Extremely Uncomfortable

31. How comfortable are you in handing over control for certain home activities to a home automation system, if you can manually change back any automatic changes made?

- ☐ Extremely comfortable
- ☐ Comfortable
- ☐ Neutral
- ☐ Uncomfortable
- ☐ Extremely Uncomfortable

Section 5: Comments

If you wish to make any comments regarding home automation, any improvements to the home automation system or aspects of this questionnaire please feel free to do so hear.

Thank you for your time and effort

Appendix B: System Evaluation: Questionnaire

Dear Respondent,

Please complete the questionnaire as honestly and descriptively as possible. The answers you provide will be vital in the successful development of home automation technology that meets users' needs. Thank you in advance for your time and effort.

Please answer ***all*** questions by ticking the appropriate box(s) unless otherwise stated.

Section 1: Personal Information

1. Gender

   ☐ Male ☐ Female

2. Age group

   ☐ Under 25 ☐ 35 – 44 ☐ 55 and over

   ☐ 25 – 34 ☐ 45 – 54

3. Based on the demonstration of the home automation system, I will adopt home automation technology in the future.

   Strongly Disagree ☐ ☐ ☐ ☐ ☐ Strongly Agree

4. Based on the demonstration of the home automation system and remote access approaches, I will want remote access to home automation devices in my home.

   Strongly Disagree ☐ ☐ ☐ ☐ ☐ Strongly Agree

Section 2: Home Gateway Defence Approach Evaluation

5. The delay in accessing and controlling devices whilst using the RHS-2 communication approach is acceptable.

   Strongly Disagree ☐ ☐ ☐ ☐ ☐ Strongly Agree

6. For non-critical, everyday, operations I am happy to use the RHS-2 communications approach.
   Strongly Disagree ☐ ☐ ☐ ☐ ☐ Strongly Agree

7. During a DDoS attack on the home automation system, the delay in switching between the RHS-2 and RHS-1 approach is acceptable.

   Strongly Disagree ☐ ☐ ☐ ☐ ☐ Strongly Agree

8. The home gateway defence approach dealt with all my requests in an efficient and effective manner before, during and after the attack.

   Strongly Disagree ☐ ☐ ☐ ☐ ☐ Strongly Agree

Section 3: Third Party Defence Approach Evaluation

9. For critical communications, I prefer to use the RHS-1 approach for communicating with a home automation system.

   Strongly Disagree ☐ ☐ ☐ ☐ ☐ Strongly Agree

10. I am happy to use the RHS-2 approach for critical applications in emergencies, when the RHS-1 approach is not available.

    Strongly Disagree ☐ ☐ ☐ ☐ ☐ Strongly Agree

11. The delay in accessing and controlling devices whilst using the RHS-1 communication approach is acceptable.

    Strongly Disagree ☐ ☐ ☐ ☐ ☐ Strongly Agree

12. During a DDoS attack on the third party, the delay in switching between the RHS-1 and RHS-2 approach is acceptable.

    Strongly Disagree ☐ ☐ ☐ ☐ ☐ Strongly Agree

13. The RHS-2 approach dealt with all my requests in an efficient and effective manner before, during and after the attack.

    Strongly Disagree ☐ ☐ ☐ ☐ ☐ Strongly Agree

Section 4: WSN DoS Defence

14. The access delay for locally controlling the WSN based HAS, during a DoS attack, with no defences provides an acceptable level of performance.

    Strongly Disagree ☐ ☐ ☐ ☐ ☐ Strongly Agree

15. The access delay for locally controlling the WSN based HAS, during a DoS attack, with existing DoS defences provides an acceptable level of performance.

    Strongly Disagree ☐ ☐ ☐ ☐ ☐ Strongly Agree

16. The access delay for locally controlling the WSN based HAS, during a DoS attack, with existing DoS defences and the proposed defences provides an acceptable level of performance.

    Strongly Disagree ☐ ☐ ☐ ☐ ☐ Strongly Agree

Section 5: System Evaluation

17. The proposed system was easy to use.

    Strongly Disagree ☐ ☐ ☐ ☐ ☐ Strongly Agree

18. I feel comfortable using the system with the different communication approaches.

    Strongly Disagree ☐ ☐ ☐ ☐ ☐ Strongly Agree

19. Based on the description and demonstration of the RHS-1 approach I am happy to use a third party to connect to a home automation system.

    Strongly Disagree ☐ ☐ ☐ ☐ ☐ Strongly Agree

20. I can effectively use the system to communicate with a home automation system.

    Strongly Disagree ☐ ☐ ☐ ☐ ☐ Strongly Agree

21. I am able to efficiently monitor and control home automation devices using the proposed system.

    Strongly Disagree ☐ ☐ ☐ ☐ ☐ Strongly Agree

22. Overall, I am happy to use such a system to communicate with my home automation system.

    Strongly Disagree ☐ ☐ ☐ ☐ ☐ Strongly Agree

Section 6: Comments

If you wish to make any comments regarding home automation, any improvements to the home automation system or aspects of this questionnaire please feel free to do so hear.

Thank you for your time and effort

Appendix C: Home Automation Test-bed Source Code

This appendices, contains the source code for the WSN based HAS test-bed introduced in Chapter 5 and used to provide a practical evaluation of the proposed DoS defence approaches presented in Chapters 6 and 7. The source code highlights the basic code structure required to program a Jennic JN5139 end node, capable of joining a ZigBee network, responding to commands (i.e. turning a light on and off), and transmitting the status of onboard sensors to the network coordinator. To implement the code, and reproduce the WSN based HAS test-bed a prior knowledge of programming for embedded devices in C, the Jennic ZigBee SDK, and the ZigBee WSN standard is required. It is important to note that the following code is provided for the repeatability of the experiments conducted in this Thesis. The following code was developed as part of the indeedNET project, and as such created by a team of which the author was one member, as discussed in Chapter 5.

Code Extract

```
/****************************************************************************
 *
 * MODULE:          Home Automation test-bed End Device code
 * VERSION:         1.05
 * DATED:           16 February 2009
 *
/****************************************************************************/
/***  The following includes references to the Jennic ZigBee SDK required by the application**/
/****************************************************************************/
#include "jendefs.h"
#include "ALSdriver.h"
#include "HTSdriver.h"
#include "AppHardwareApi.h"
#include "LedControl.h"
#include "Button.h"
#include "gdb.h"
#include "JZ_Api.h"
#include "AppApi.h"
#include "HomeDemoProfile.h"
#include "nwk.h"
#include "Utils.h"
/****************************************************************************/
/***       Definitions                                                    ***/
/****************************************************************************/
/* Timing values */
#define ONE_SEC_IN_32K_PERIODS 32000UL
#define HW_INT_Q_SIZE         32
#define HW_INT_Q_PTR_MASK     0x1f
#define TX_WAIT_MS            20
//#define SLEEP_PERIOD_ms       250UL
//#define SLEEP_PERIOD          (SLEEP_PERIOD_ms * 32UL)
/****************************************************************************/
/***       Type Definitions                                               ***/
/****************************************************************************/
/* State machine states */
typedef enum
{
  E_STATE_READY_TO_READ_SENSORS,
  E_STATE_READING_S1,
```

```
   E_STATE_READING_S2
} teState;

typedef struct
{
   uint32 u32Device;
   uint32 u32ItemBitmap;
} tsHwIntData;

/* All variables with scope throughout module are in one structure */
typedef struct
{
   /* Transceiver (basically anything TX/RX not covered elsewhere) */
   struct
   {
      uint8   u8CurrentTxHandle;
      uint8   u8PrevRxBsn;
   } sTransceiver;

   /* Controls (switch, light level alarm) */
   struct
   {
      uint8   u8Switch;
      uint8   u8LedState;
   } sControls;

   /* Sensor data, stored between read and going out in frame */
   struct
   {
      uint8   u8TempResult;
      uint8   u8HtsResult;
      uint8   u8AlsResult;
   } sSensors;

   /* System (state, assigned address, channel) */
   struct
   {
      teState eState;
      uint8   u8Channel;
      uint32  u32CalibratedTimeout;
   } sSystem;

   /* Queue for hardware interrupts */
   struct
   {
      tsHwIntData    asHwIntData[HW_INT_Q_SIZE];
      volatile uint8 u8ReadPtr;
      volatile uint8 u8WritePtr;
   } sQueue;

   bool_t bJoined;
   bool_t bRejoining;

} tsDemoData;

/****************************************************************************/
/***        Local Function definitions                                    ***/
/****************************************************************************/
PRIVATE void  vInitDemoSystem(bool_t bColdStart);
```

```
PRIVATE void  vInitEndpoint(void);
PRIVATE void  vStartReadSensors(void);
PRIVATE void  vReadSensor2(void);
PRIVATE void  vReadSensor3(void);
PRIVATE void  vSendData(uint8 u8LightValue, uint8 u8TempValue,
                uint8 u8HumidityValue, uint8 u8Switch);
PRIVATE uint8 u8FindMin(uint8 u8Val1, uint8 u8Val2);
PRIVATE void  vSleep(void);
PRIVATE void  vAddDesc(void);
#ifdef TEST_BOS_TIMER
PRIVATE void vTimerFired0(void *pvMessage, uint8 u8Len);
PRIVATE void vTimerFired1(void *pvMessage, uint8 u8Len);
#endif
PRIVATE void  vSendDatab(uint16 u16Addr,uint8 ID, uint8 u8LightValue, uint8 u8TempValue,
                uint8 u8HumidityValue, uint8 u8Switch);

/****************************************************************************/
/***        Local Variables                                               ***/
/****************************************************************************/
tsDemoData sDemoData;
#ifdef TEST_BOS_TIMER
uint8 u8LedFlash0 = 0;
uint8 u8LedFlash1 = 0;
#endif

/****************************************************************************
 *
 * NAME: AppColdStart
 *
 * DESCRIPTION:
 * Entry point for application. Initialises system, starts scan then
 * processes interrupts.
 *
 * RETURNS:
 * void, never returns
 *
 ****************************************************************************/
PUBLIC void AppColdStart(void)
{
   /* Debug hooks: include these regardless of whether debugging or not */
   HAL_GDB_INIT();
   HAL_BREAKPOINT();

   /* General initialisation: reset hardware */
   JZS_sConfig.u32Channel = 0;
   JZS_sConfig.u16PanId = DEMO_PAN_ID;
   JZS_sConfig.u16AppDataLength = 0;

   vInitDemoSystem(TRUE);

   /* No return from the above function call */
}

/****************************************************************************
 *
 * NAME: AppWarmStart
 *
 * DESCRIPTION:
 * Entry point for application from boot loader. Simply jumps to AppColdStart
```

```
 * as, in this instance, application will never warm start.
 *
 * RETURNS:
 * Never returns.
 *
 ****************************************************************************/
PUBLIC void AppWarmStart(void)
{
   vInitDemoSystem(FALSE);
}

/****************************************************************************
 *
 * NAME: JZA_boAppStart
 *
 * DESCRIPTION:
 * Called by Zigbee stack during initialisation. Sets up the profile
 * information and starts the networking activity
 *
 * RETURNS:
 * TRUE
 *
 ****************************************************************************/
PUBLIC bool_t JZA_boAppStart(void)
{
#ifdef TEST_BOS_TIMER
   bBosCreateTimer(vTimerFired0, NULL, 0, 10, NULL);
   bBosCreateTimer(vTimerFired1, NULL, 0, 15, NULL);
#endif

   JZS_vStartStack();
   return TRUE;
}

/****************************************************************************
 *
 * NAME: JZA_eAfKvpObject
 *
 * DESCRIPTION:
 * Receives incoming KVP data frames
 *
 * PARAMETERS:      Name              RW  Usage
 *              eAddrMode          R   Address mode of incoming frame
 *              u16AddrSrc         R   Network address of source node
 *              u8SrcEP            R   Endpoint address of source node
 *              u8LQI              R   Link Quality Indication
 *              u8DstEP            R   Destination endpoint address
 *              u8ClusterId        R   Cluster ID of incoming frame
 *              *pu8ClusterIDRsp   R   Pointer to cluster ID of response frame
 *              *puTransactionInd  R   Pointer to incoming frame
 *              *puTransactionRsp  R   Pointer to response frame
 *
 * RETURNS:
 * TRUE for stack to automatically generate KVP response frames when appropriate
 * FALSE otherwise
 *
 ****************************************************************************/
PUBLIC bool_t JZA_bAfKvpObject( APS_Addrmode_e         eAddrMode,
                        uint16                 u16AddrSrc,
```

```
                        uint8               u8SrcEP,
                        uint8               u8LQI,
                        uint8               u8DstEP,
                        uint8               u8ClusterId,
                        uint8               *pu8ClusterIDRsp,
                        AF_Transaction_s    *puTransactionInd,
                        AF_Transaction_s    *puTransactionRsp)
{
        bool_t bReturnVal = FALSE;
/*
        if (puTransactionInd->uFrame.sKvp.eCommandTypeID == SET_ACKNOWLEDGMENT)
        {
                bReturnVal = TRUE;
        }

   if ((eAddrMode != APS_ADDRMODE_SHORT) || (u8DstEP != 0x40))
   {
      puTransactionRsp->uFrame.sKvp.eErrorCode = KVP_INVALID_ENDPOINT;
      return bReturnVal;
   }

   if (    (puTransactionInd->uFrame.sKvp.eCommandTypeID != SET)
      &&  (puTransactionInd->uFrame.sKvp.eCommandTypeID != SET_ACKNOWLEDGMENT))
   {
      puTransactionRsp->uFrame.sKvp.eErrorCode = KVP_INVALID_COMMAND_TYPE;
      return bReturnVal;
   }

 // Assume data is switch info, and set LED based on the received command //
 sDemoData.sControls.u8LedState = puTransactionInd->uFrame.sKvp.uAttributeData.UnsignedInt8;
vLedControl(0, sDemoData.sControls.u8LedState);

   puTransactionRsp->uFrame.sKvp.eErrorCode =  KVP_SUCCESS;
   return bReturnVal;
*/

   uint8   *pu8Afdu;
   uint8   u8Length;
   int i;
   uint64 u64DeviceAddr = 0;
   uint64 u64Temp = 0;
   bool_t boFound;

if (puTransactionInd->uFrame.sKvp.eCommandTypeID == SET_ACKNOWLEDGMENT)
        {
                bReturnVal = TRUE;
        }

   u8Length = puTransactionInd->uFrame.sKvp.uAttributeData.CharacterString.u8CharacterCount;
   pu8Afdu = puTransactionInd->uFrame.sKvp.uAttributeData.CharacterString.au8CharacterData;

   if ((eAddrMode != APS_ADDRMODE_SHORT) || (u8DstEP != 0x40))
   {
      puTransactionRsp->uFrame.sKvp.eErrorCode = KVP_INVALID_ENDPOINT;
      return bReturnVal;
   }

   if (    (puTransactionInd->uFrame.sKvp.eCommandTypeID != SET)
      &&  (puTransactionInd->uFrame.sKvp.eCommandTypeID != SET_ACKNOWLEDGMENT))
```

```
   {
      puTransactionRsp->uFrame.sKvp.eErrorCode = KVP_INVALID_COMMAND_TYPE;
      return bReturnVal;
   }


   pu8Afdu++;

   if(puTransactionInd->uFrame.sKvp.u16AttributeID == DAP_ATTR_SENSOR_DATA)
   {
      /* Search for address in list */
      boFound = FALSE;

      for (i = 0; i < 7; i++)
      {
         u64DeviceAddr = u64DeviceAddr << 8;
         u64DeviceAddr |= *pu8Afdu++;
      }
   }

      uint8 Address = 0;

      Address  = *pu8Afdu++;

//Send an acknowledgment back to the device which sent the message to change the status of the
//connected light, together with the sensor readings, including the current status of the light.

vSendData(101,255,Address,254);

   puTransactionRsp->uFrame.sKvp.eErrorCode = KVP_INVALID_COMMAND_TYPE;
            return bReturnVal;

}

/****************************************************************************
 *
 * NAME: JZA_vAfKvpResponse
 *
 * DESCRIPTION:
 * Used to send response to incoming KVP frame
 *
 * PARAMETERS:      Name              RW  Usage
 *                  eAddrMode         R   Address mode of incoming frame
 *                  u16AddrSrc        R   Network address of source node
 *                  u8SrcEP           R   Endpoint address of source node
 *                  u8LQI             R   Link Quality Indication
 *                  u8DstEP           R   Destination endpoint address
 *                  u8ClusterId       R   Cluster ID of incoming frame
 *                  *puTransactionInd R   Pointer to incoming frame
 *
 * RETURNS:
 * void
 *
 ****************************************************************************/
PUBLIC void JZA_vAfKvpResponse(APS_Addrmode_e         eAddrMode,
                        uint16                u16AddrSrc,
                        uint8                 u8SrcEP,
                        uint8                 u8LQI,
                        uint8                 u8DstEP,
```

```
                    uint8               u8ClusterID,
                    AF_Transaction_s    *puTransactionInd)
{

}

/************************************************************************
 *
 * NAME: JZA_pu8AfMsgObject
 *
 * DESCRIPTION:
 * Receives incoming MSG data frames.
 *
 * PARAMETERS:      Name                RW  Usage
 *              eAddrMode           R   Address mode of incoming frame
 *              u16AddrSrc          R   Network address of source node
 *              u8SrcEP             R   Endpoint address of source node
 *              u8LQI               R   Link Quality Indication
 *              u8DstEP             R   Destination endpoint address
 *              u8ClusterId         R   Cluster ID of incoming frame
 *              *pu8ClusterIDRsp    R   Pointer to cluster ID of response frame
 *              *puTransactionInd   R   Pointer to incoming frame
 *              *puTransactionRsp   R   Pointer to response frame
 * RETURNS:
 * FALSE
 *
 ************************************************************************/
PUBLIC bool_t JZA_bAfMsgObject(APS_Addrmode_e       eAddrMode,
                    uint16              u16AddrSrc,
                    uint8               u8SrcEP,
                    uint8               u8LQI,
                    uint8               u8DstEP,
                    uint8               u8ClusterID,
                    uint8               *pu8ClusterIDRsp,
                    AF_Transaction_s    *puTransactionInd,
                    AF_Transaction_s    *puTransactionRsp)
{
  return FALSE;
}


/************************************************************************
 *
 * NAME: JZA_vZdpResponse
 *
 * DESCRIPTION:
 * Called when a ZDP response frame has been received. In this case no action
 * is taken as no ZDP responses are anticipated.
 *
 * PARAMETERS:      Name            RW  Usage
 *              u8Type          R   ZDP response type
 *              pu8Payload      R   Payload buffer
 *              u8PayloadLen    R   Length of payload
 *
 ************************************************************************/
PUBLIC void JZA_vZdpResponse(uint8 u8Type, uint8 u8Lqi, uint8 *pu8Payload,
                    uint8 u8PayloadLen)
{
}
```

```
/****************************************************************************
 *
 * NAME: JZA_vAppEventHandler
 *
 * DESCRIPTION:
 * Called regularly by the task scheduler. This function reads the hardware
 * event queue and processes the events therein. It is important that this
 * function exits after a relatively short time so that the other tasks are
 * not adversely affected.
 *
 ****************************************************************************/
PUBLIC void JZA_vAppEventHandler(void)
{
   tsHwIntData *psHwIntData;
   static bool_t bEBStatus = 0;

   if(!bEBStatus)
   {
      if (sDemoData.bJoined == TRUE)
      {
         /* Things to do when first called */
         //vStartReadSensors(); /* Now done upon successful joining */

         vLedControl(1, FALSE);

         bEBStatus = TRUE;
      }
   }

   /* Check queue for hardware interrupts, and process */
   while (sDemoData.sQueue.u8WritePtr != sDemoData.sQueue.u8ReadPtr)
   {
      psHwIntData
         = &sDemoData.sQueue.asHwIntData[sDemoData.sQueue.u8ReadPtr];

      switch (psHwIntData->u32Device)
      {
      case E_AHI_DEVICE_SYSCTRL:
         /* Check for DIO pin used by humidity/temperature sensor */
         if (psHwIntData->u32ItemBitmap & HTS_DATA_DIO_BIT_MASK)
         {
            switch (sDemoData.sSystem.eState)
            {
            case E_STATE_READING_S1:
               vReadSensor2();
               break;

            case E_STATE_READING_S2:
               vReadSensor3();
               break;

            default:
               break;
            }
         }

         /* Check for wake timer */
         if (psHwIntData->u32ItemBitmap & (1 << E_AHI_SYSCTRL_WK1))
```

```
        {
          /* Only restart sensor reading if not rejoining (if rejoining,
            sensor reading will be restarted when that is complete) */
          if (sDemoData.bRejoining == FALSE)
          {
            vStartReadSensors();
          }
        }

        /* Check for buttons */
        if (psHwIntData->u32ItemBitmap
          & (BUTTON_ALL_MASK_RFD << BUTTON_BASE_BIT))
        {
          uint8 u8KeysDown
            = (uint8)(psHwIntData->u32ItemBitmap >> BUTTON_BASE_BIT);

          switch (u8KeysDown)
          {
          case BUTTON_0_MASK:
            sDemoData.sControls.u8Switch = 0;
            break;

          case BUTTON_1_MASK:
            sDemoData.sControls.u8Switch = 1;
            break;
          }
        }
        break;

      default:
        break;
      }

      sDemoData.sQueue.u8ReadPtr
        = (sDemoData.sQueue.u8ReadPtr + 1) & HW_INT_Q_PTR_MASK;
    }
}

/****************************************************************************
 *
 * NAME: JZA_vPeripheralEvent
 *
 * DESCRIPTION:
 * Called when a hardware event causes an interrupt. This function is called
 * from within the interrupt context so should be brief. In this case, the
 * information is placed on a simple FIFO queue to be processed later.
 *
 * PARAMETERS: Name          RW  Usage
 *           u32Device     R   Peripheral generating interrupt
 *           u32ItemBitmap R   Bitmap of interrupt sources within peripheral
 *
 ****************************************************************************/
PUBLIC void JZA_vPeripheralEvent(uint32 u32Device, uint32 u32ItemBitmap)
{
  tsHwIntData *psHwIntData;
  uint8       u8WriteNextPtr;

  /* Queue event for processing during appKeyOperationKey call */
```

```
   u8WriteNextPtr = (sDemoData.sQueue.u8WritePtr + 1) & HW_INT_Q_PTR_MASK;

   if (u8WriteNextPtr != sDemoData.sQueue.u8ReadPtr)
   {
      /* There is space on queue */
      psHwIntData
         = &sDemoData.sQueue.asHwIntData[sDemoData.sQueue.u8WritePtr];
      psHwIntData->u32Device = u32Device;
      psHwIntData->u32ItemBitmap = u32ItemBitmap;

      sDemoData.sQueue.u8WritePtr = u8WriteNextPtr;
   }

   /* If no space on queue, interrupt is silently discarded */
}

/****************************************************************************
 *
 * NAME: JZA_vStackEvent
 *
 * DESCRIPTION:
 * Called when a miscellaneous stack event occurs.
 *
 * PARAMETERS:      Name          RW  Usage
 *                  eEventId      R   Event enumeration
 *                  puStackEvent  R   Event information
 *
 * RETURNS:
 * NULL
 *
 ****************************************************************************/
PUBLIC void JZA_vStackEvent(teJZS_EventIdentifier eEventId,
                    tuJZS_StackEvent *puStackEvent)
{
   switch (eEventId)
   {
   case JZS_EVENT_APS_DATA_CONFIRM:
      if (puStackEvent->sApsDataConfirmEvent.u8Status != 0)
      {
         if (sDemoData.bRejoining == FALSE)
         {
            sDemoData.bJoined = FALSE;
            sDemoData.bRejoining = TRUE;

            /* Try to re-join network: timer will send a frame again in a
               second */
            JZS_vRejoinNetwork();
         }
      }
      else
      {
         if (sDemoData.bRejoining == FALSE)
         {
            /* Go to sleep: sleep itself will not be scheduled until BOS
               has completed any other actions */
            vSleep();
         }
      }
      break;
```

```
    case JZS_EVENT_NWK_JOINED_AS_ENDDEVICE:
        vAddDesc();
        sDemoData.bJoined = TRUE;
        sDemoData.bRejoining = FALSE;
        vStartReadSensors();

        /* Note: can use puStackEvent->sNwkJoinedEvent.u16Addr to detect if
           device address has changed */

        break;

    default:
        break;
    }
}

/****************************************************************************
 *
 * NAME: vInitDemoSystem
 *
 * DESCRIPTION:
 * Initialises Zigbee stack and hardware. Final action is to start BOS, from
 * which there is no return. Subsequent application actions occur in the
 * functions defined above.
 *
 * RETURNS:
 * No return from this function
 *
 ****************************************************************************/
PRIVATE void vInitDemoSystem(bool_t bColdStart)
{
    /* Initialise software elements */
    vInitEndpoint();

#if 1
    vAHI_UartEnable(E_AHI_UART_0);
    vAHI_UartReset(E_AHI_UART_0, TRUE, TRUE);
    vAHI_UartSetClockDivisor(E_AHI_UART_0, E_AHI_UART_RATE_19200);   //38400
    vAHI_UartReset(E_AHI_UART_0, FALSE, FALSE);
#endif

    /* Initialise Zigbee stack */
    (void)JZS_u32InitSystem(bColdStart);

    /* Set DIO for buttons and LEDs. Also, if waking up, set up the
       BOS into the correct state */
    if (bColdStart == TRUE)
    {
        vLedControl(0, TRUE);
    }

    vLedControl(1, TRUE);
    vLedInitRfd();
    vButtonInitRfd();

    /* Enable interrupts for DIO buttons */
    vAHI_DioWakeEdge(0, BUTTON_ALL_MASK_RFD << BUTTON_BASE_BIT);
    vAHI_DioWakeEnable(BUTTON_ALL_MASK_RFD << BUTTON_BASE_BIT, 0);
```

```
   /* Set up interrupt for humidity/temp sensor (don't enable yet) */
   vAHI_DioWakeEdge(0, HTS_DATA_DIO_BIT_MASK);

   /* Set up peripheral hardware */
   vALSreset();
   vHTSreset();

   /* Start ALS now: it automatically keeps re-sampling after this */
   vALSstartReadChannel(0);

   /* Enable timer to use for sequencing */
   if (bColdStart == TRUE)
   {
      /* Calibrate wake timer */
      sDemoData.sSystem.u32CalibratedTimeout
         = ONE_SEC_IN_32K_PERIODS * 10000 / u32AHI_WakeTimerCalibrate();
      vAHI_WakeTimerEnable(E_AHI_WAKE_TIMER_1, TRUE);
   }

   /* Start BOS */
   bBosRun(bColdStart);
}

/****************************************************************************
 *
 * NAME: vSendData
 *
 * DESCRIPTION:
 * Generates and sends a frame consisting of 4 KVP transactions, for the four
 * values that are passed to the controller.
 *
 * PARAMETERS: Name            RW  Usage
 *          u8LightValue     R   Value from light sensor
 *          u8TempValue      R   Value from temperature sensor
 *          u8HumidityValue  R   Value from humidity sensor
 *          u8Switch         R   Switch value (0 or 1)
 *
 ****************************************************************************/
PRIVATE void vSendData(uint8 u8LightValue, uint8 u8TempValue,
                uint8 u8HumidityValue, uint8 u8Switch)
{
   uint8             u8SrcEP = 0x30;
   AF_Transaction_s    Transaction;
   APS_Addrmode_e      eAddrMode;
   uint16             u16DestAddr;
   uint8             u8DestEndpoint;
   uint8            *pu8Afdu;
   uint8             transCount = 1;
   uint8             *pu8ExtAdr;
   uint8             i;
#if 0
   uint8             u8TimerID;
#endif

   /* Set pointer to point to location in internal RAM where extended addres  is stored */
   pu8ExtAdr = (uint8 *)pvAppApiGetMacAddrLocation();

   eAddrMode = APS_ADDRMODE_SHORT;
```

```
   u16DestAddr = 0x0000;
   u8DestEndpoint = 0x40;

   Transaction.u8SequenceNum = u8AfGetTransactionSequence(TRUE);
   Transaction.uFrame.sKvp.eErrorCode = KVP_SUCCESS;
   Transaction.uFrame.sKvp.eCommandTypeID = SET;
   Transaction.uFrame.sKvp.eAttributeDataType = KVP_CHARACTER_STRING;
   Transaction.uFrame.sKvp.u16AttributeID = DAP_ATTR_SENSOR_DATA;
   Transaction.uFrame.sKvp.uAttributeData.CharacterString.u8CharacterCount = 13;

   pu8Afdu = Transaction.uFrame.sKvp.uAttributeData.CharacterString.au8CharacterData;

   /* Set length field */
   pu8Afdu[0] = 12;

   /* Load extended address into frame payload */
   for (i = 0; i < 8; i++)
   {
      pu8Afdu[i + 1] = *(pu8ExtAdr + i);
   }

   /* Load sensor data into frame payload */
   pu8Afdu[9]  = u8LightValue;
   pu8Afdu[10] = u8TempValue;
   pu8Afdu[11] = u8HumidityValue;
   pu8Afdu[12] = u8Switch;

   afdeDataRequest(eAddrMode,
               u16DestAddr,
               u8DestEndpoint,
               u8SrcEP,
               DAP_PROFILE_ID,
               DAP_CID_SENSOR_READINGS,
               AF_KVP,
               transCount,
               &Transaction,
               APS_TXOPTION_NONE,
               ENABLE_ROUTE_DISCOVERY,
               0);

   vSleep();

}

/****************************************************************************
 *
 * NAME: vStartReadSensors/vReadSensor2/vReadSensor3
 *
 * DESCRIPTION:
 * Gets the current readings from each sensor. Uses the DIO line for the HTS
 * sensor to signal when a value is ready to be read, as this allows the CPU
 * to doze during the reading calculation.
 *
 * RETURNS:
 * void
 *
 ****************************************************************************/
PRIVATE void vStartReadSensors(void)
{
```

```
   sDemoData.sSystem.eState = E_STATE_READING_S1;

   /* Set wake timer for the next time that we want to read the sensors */
   vAHI_WakeTimerStart(E_AHI_WAKE_TIMER_1,
                  sDemoData.sSystem.u32CalibratedTimeout * 1);

   /* Start to read temperature */
   vHTSstartReadTemp();

   /* Enable interrupt on DIO to tell when read has completed */
   vAHI_DioWakeEnable(HTS_DATA_DIO_BIT_MASK, 0);
}

PRIVATE void vReadSensor2(void)
{
   sDemoData.sSystem.eState = E_STATE_READING_S2;

   /* Clear interrupt on DIO */
   vAHI_DioWakeEnable(0, HTS_DATA_DIO_BIT_MASK);

   /* Read temperature, 0-52 are acceptable */
   sDemoData.sSensors.u8TempResult
      = u8FindMin((uint8)u16HTSreadTempResult(), 52);

   /* Start to read humidity */
   vHTSstartReadHumidity();

   /* Enable interrupt on DIO to tell when read has completed */
   vAHI_DioWakeEnable(HTS_DATA_DIO_BIT_MASK, 0);
}

PRIVATE void vReadSensor3(void)
{
   /* Clear interrupt on DIO */
   vAHI_DioWakeEnable(0, HTS_DATA_DIO_BIT_MASK);

   /* Read humidity, 0-104 are acceptable */
   sDemoData.sSensors.u8HtsResult
      = u8FindMin((uint8)u16HTSreadHumidityResult(), 104);

   /* Read light level, adjust to range 0-6 in a slightly non-linear way */
   sDemoData.sSensors.u8AlsResult
      = u8FindMin((uint8)(u16ALSreadChannelResult() >> 6), 6);

   /* Send the frame */
   vSendData(sDemoData.sSensors.u8AlsResult,
         sDemoData.sSensors.u8TempResult,
         sDemoData.sSensors.u8HtsResult,
         sDemoData.sControls.u8LedState);
}

/****************************************************************************
 * NAME: vInitEndpoint
 * DESCRIPTION:
 * Initialises software structures and variables.
 * RETURNS:
 * void
 ****************************************************************************/
PRIVATE void vInitEndpoint(void)
```

```
{
   /* Set defaults for software */
   sDemoData.sTransceiver.u8CurrentTxHandle = 0;
   sDemoData.sControls.u8Switch = 0;
   sDemoData.sSensors.u8TempResult = 0;
   sDemoData.sSensors.u8HtsResult = 0;
   sDemoData.sSensors.u8AlsResult = 0;
   sDemoData.sSystem.eState = E_STATE_READY_TO_READ_SENSORS;
   sDemoData.sQueue.u8ReadPtr = 0;
   sDemoData.sQueue.u8WritePtr = 0;
   sDemoData.bJoined = FALSE;
   sDemoData.bRejoining = FALSE;
}
/****************************************************************************
 *
 * NAME: vAddDesc
 *
 * DESCRIPTION:
 * Initialises software structures and variables.
 *
 * RETURNS:
 * void
 *
 ****************************************************************************/
PRIVATE void vAddDesc(void)
{
   /* Sensor has 1 endpoint, only expects data from coordinator */
   uint8  u8DeviceVer = 0x00;
   uint8  u8Flags = 0x00;
   uint8  u8EndPoint = 0x40;
   uint16 u16DeviceId = 0x0000;

   uint8 u8InputClusterCnt = 1;
   uint8 au8InputClusterList[] = {DAP_CID_SWITCH};
   uint8 u8OutputClusterCnt = 0;
   uint8 au8OutputClusterList[] = {};

   (void)afmeSimpleDescAdd(u8EndPoint, DAP_PROFILE_ID, u16DeviceId,
                     u8DeviceVer, u8Flags, u8InputClusterCnt,
                     au8InputClusterList, u8OutputClusterCnt,
                     au8OutputClusterList);
}
/****************************************************************************
 *
 * NAME: u8FindMin
 *
 * DESCRIPTION:
 * Returns the smallest of two values.
 *
 * PARAMETERS:      Name    RW  Usage
 *                  u8Val1  R   First value to compare
 *                  u8Val2  R   Second value to compare
 *
 * RETURNS:
 * uint8, lowest of two input values
 *
 ****************************************************************************/
PRIVATE uint8 u8FindMin(uint8 u8Val1, uint8 u8Val2)
{
```

```
   if (u8Val1 < u8Val2)
   {
      return u8Val1;
   }
   return u8Val2;
}
/****************************************************************************
 *
 * NAME: vSleep
 *
 * DESCRIPTION: Sends device to light sleep.
 *
 * RETURNS:
 * void
 *
 ****************************************************************************/
PRIVATE void vSleep(void)
{
#if 0 /* Enable sleep operation: if #if 0, everything still works but never
        sleeps */

   /* Turn off LEDs to save power */
   vLedControl(0, FALSE);
   vLedControl(1, FALSE);

   /* Power down: device will wake up from wake timer 1, which was set
      in vStartReadSensors */
   vBosRequestSleep(TRUE);
#endif
}

#ifdef TEST_BOS_TIMER
PRIVATE void vTimerFired0(void *pvMessage, uint8 u8Len)
{
   uint8 u8Dummy;

   u8LedFlash0 = 1 - u8LedFlash0;
   vLedControl(0, u8LedFlash0);

   bBosCreateTimer(vTimerFired0, NULL, 0, 10, &u8Dummy);
}

PRIVATE void vTimerFired1(void *pvMessage, uint8 u8Len)
{
   uint8 u8Dummy;

   u8LedFlash1 = 1 - u8LedFlash1;
   vLedControl(1, u8LedFlash1);

   bBosCreateTimer(vTimerFired1, NULL, 0, 15, &u8Dummy);
}
#endif

/****************************************************************************/
/***        END OF FILE                                                   ***/
/****************************************************************************/
```

Appendix D: RHS-1 and RHS-2 Source Code

This appendices, contains the source code used for the establishment of both the RHS-1 and RHS-2 code.

RHS-1 Approach, Mobile Client Source Code

```
////////////////////////////////////////////////////////////////////////////////
// Local Variables                                                            //
////////////////////////////////////////////////////////////////////////////////

private StreamConnection streamConnection = null;
private OutputStream outputStream = null;
private DataOutputStream dataOutputStream = null;
private InputStream inputStream = null;
private DataInputStream dataInputStream = null;
private String connectString = "socket://192.168.0.102:11000";  //The fixed address of the RHS

private byte[] K1 = Hex.decode("404142434445464748494a4b4c4d4e4f");
private byte[] N1 = Hex.decode("101112131415161718191a1b1c");

private byte[] K2 = Hex.decode("303132333435363738393a3b3c3d3e3f");
private byte[] N2 = Hex.decode("202122232425262728292a2b2c");

private byte [] sessionKey;
private byte [] AESinitV;
private int randomNumber;

private byte [] sessionKey2;
private byte [] AESinitV2;

private int randomNumber2;

private byte[] enc;
private int len;

 ////////////////////////////////////////////////////////////////////////////////
////////////////////////////////////////////////////////////////////////////////

////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////
//The login code – connects to the RHS using a pre-shared key, request a session key, then sends a //
//a new dual encrypted session key directly to the WSN based HAS                                    //
////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////

   public void login(String userName, String userPassword){

            millsStart = System.currentTimeMillis();

        String loginStatus = Home.login(userName, userPassword);

         if(!loginStatus.equals("-1")){

           String data = "";
           String testData = "";
           HomeID = loginStatus;
```

```
            data = Home.RequestSessionKey();
            testData = Home.sendSessionKey(HomeID);
            System.out.println(data);
            MainMenu();

             //Load the local database with sensor readings
             sensorDatabase();
         }else if(loginStatus.equals("-1")){
             loginStatuslbl.setText("The login detailes you provided were incorrect, please try
again.\n\n ");
         }else{
         message("Critical Login Error Recived: " + loginStatus);
         }
    }
////////////////////////////////////////////////////////////////////////////////
////////////////////////////////////////////////////////////////////////////////

////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////
//The login function encrypts the user username and password and sends it to the RHS for              //
//authentication, if the RHS can establish a connection on behalf of the mobile client with the WSN//
//based HAS, the RHS returns that the login is successful                                            //
////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////

   public String Home.login(String userName, String userPassword){

      StringBuffer results = new StringBuffer();
      String resultField = "No data recived";

      try{

         streamConnection = (StreamConnection) Connector.open(connectString);
         outputStream = streamConnection.openOutputStream();
         dataOutputStream = new DataOutputStream(outputStream);

         byte[] byteMessage = Encrypt(true,("<lgn>" + "," + userName + "," + userPassword + "," +
"<EOF>"),K1,N1);

         int x = 0;

         while(x < (byteMessage.length) ){
            dataOutputStream.writeByte(byteMessage[x]);
            //System.out.println(byteMessage[x]);
            x++;
         }

         //Prints a comma
         dataOutputStream.writeByte(44);

         //Prints <EOF> at the end of string to end conection
         dataOutputStream.writeByte(60);
         dataOutputStream.writeByte(69);
         dataOutputStream.writeByte(79);
         dataOutputStream.writeByte(70);
         dataOutputStream.writeByte(62);
         dataOutputStream.flush();
         inputStream = streamConnection.openInputStream();
         dataInputStream = new DataInputStream(inputStream);

         int inputChar;
```

```
            while((inputChar = dataInputStream.read()) != -1){
               results.append((char) inputChar);
            }

            resultField = new String(results.toString());

         }catch(IOException e){
            System.err.println("Exception Caught:" + e);
         }finally{

               try{
                  if(dataInputStream != null){
                  dataInputStream.close();
                  }
               }catch(IOException ignored){};

               try{
                  if(dataOutputStream != null){
                  dataOutputStream.close();
                  }
               }catch(IOException ignored){};

               try{
                  if(outputStream != null){
                  outputStream.close();
                  }
               }catch(IOException ignored){};

               try{
                   if(inputStream != null){
                  inputStream.close();
                  }
               }catch(IOException ignored){};

               try{
                   if(streamConnection != null){
                  streamConnection.close();
                  }
               }catch(IOException ignored){};
         }

            String loginStatus = resultField.trim();
            return loginStatus;

      }

////////////////////////////////////////////////////////////////////////////////
////////////////////////////////////////////////////////////////////////////////

//////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////
//The request session key function , requests a session key from the RHS, decrypts the retuned        //
//session key and uses the key for all future communications with the RHS for the current              //
//communication session.                                                                               //
//////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////
      public String RequestSessionKey(){

         StringBuffer results = new StringBuffer();
         String resultField = "No session key recived";
```

```
//Generate a random number and store in the global randomNumber variable
Random generator = new Random();
generator.setSeed(System.currentTimeMillis());

randomNumber = generator.nextInt(10000000);

while(randomNumber < 0){
   randomNumber = generator.nextInt(10000000);
}

String randomNumberString = Integer.toHexString(randomNumber);
byte[] rand = randomNumberString.getBytes();
byte[] cmd =  "<KEY>,".getBytes();
byte[] end = ",<EOF>".getBytes();
byte[] comma = ",".getBytes();
byte[] rawData = new byte[cmd.length + rand.length + end.length];

   int p = 0;

   while(p < cmd.length){
      rawData[p] = cmd[p];
      p++;
   }

   int o = 0;

   while(o < rand.length){
      rawData[p] = rand[o];
      o++;
      p++;
   }

   int q = 0;

   while(q < end.length){
      rawData[p] = end[q];
      q++;
      p++;
   }

 byte[] byteMessage = EncryptByte(true,(rawData));

try{

   streamConnection = (StreamConnection) Connector.open(connectString);
   outputStream = streamConnection.openOutputStream();
   dataOutputStream = new DataOutputStream(outputStream);

   int x = 0;

   while(x < (byteMessage.length) ){
      dataOutputStream.writeByte(byteMessage[x]);
      //System.out.println(byteMessage[x]);
      x++;
   }


   //Prints a comma to seperate parameters
```

```
    dataOutputStream.writeByte(44);

    //Prints <EOF> at the end of string to end conection
    dataOutputStream.writeByte(60);
    dataOutputStream.writeByte(69);
    dataOutputStream.writeByte(79);
    dataOutputStream.writeByte(70);
    dataOutputStream.writeByte(62);

    dataOutputStream.flush();

    inputStream = streamConnection.openInputStream();
    dataInputStream = new DataInputStream(inputStream);

    int inputChar;

    while((inputChar = dataInputStream.read()) != -1){
       results.append((char) inputChar);
    }

    resultField = new String(results.toString());


 }catch(IOException e){
    System.err.println("Exception Caught:" + e);
 }finally{

       try{
          if(dataInputStream != null){
          dataInputStream.close();
          }
       }catch(IOException ignored){};

       try{
          if(dataOutputStream != null){
          dataOutputStream.close();
          }
       }catch(IOException ignored){};

       try{
          if(outputStream != null){
          outputStream.close();
          }
       }catch(IOException ignored){};

       try{
           if(inputStream != null){
          inputStream.close();
          }
       }catch(IOException ignored){};

       try{
           if(streamConnection != null){
          streamConnection.close();
          }
       }catch(IOException ignored){};
 }

      String data = "";
```

```
            data = Decrypt_v2(false, resultField);

            private byte [] sessionKey;
             private byte [] AESinitV;
             private int randomNumber;

            String IVtest = new String(data.substring(data.length()-26,data.length()));
           String keytest = new String(data.substring(data.length()-26-34,data.length()-28));
            String recievedNonceHex = new String(data.substring(0,data.length()-26-36));
            int NonceTest = Integer.parseInt(recievedNonceHex,16);

            if(NonceTest == (randomNumber+1)){
                resultField = "Session Keys Shared";
                sessionKey = Hex.decode(keytest);
                AESinitV = Hex.decode(IVtest);
            }else{
                resultField = "Failed to Share Session Keys";
            }

           return resultField;

    }

////////////////////////////////////////////////////////////////////////////////
////////////////////////////////////////////////////////////////////////////////


////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////
//The send session key function is used to generate a session key, encrypt it with the pre-shared      //
//client master key, add routing information and encrypt it again using the sever mater session key //
//and send it to the RHS for redirection to the WSN based HAS                                                                  //
////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////

public String sendSessionKey(String HomeID){
        try{
          generateAESKey(); //called to initialise the keys and IV
        }catch(Exception e){
           System.out.println("error generating AES key");
        }

         byte[] keyBytes = Hex.encode(sessionKey2);
         String hexKey = new String(keyBytes);

         byte[] IVBytes = Hex.encode(AESinitV2);
         String hexIV = new String(IVBytes);

         int rand = 8;
         String randString = Integer.toHexString(rand);

         //There is a size limit to the length of data that the aes coprocessor can decrypt on the zigbee
        //nodes so data needs to be split into the appropriate sized packets and reassembled on the
        //ZigBee node. The substring in j2me is (start index, end index - 1)

         String tempA = "<SK1>," + randString + hexKey.substring(0,12) + ",<EOF>";
         String tempB = "<SK2>," + randString + hexKey.substring(12,24) + ",<EOF>";
         String tempC = "<SK3>," + randString + hexKey.substring(24,32) + ",<EOF>";
         String tempD = "<SN1>," + randString + hexIV.substring(0,13) + ",<EOF>";
         String tempE = "<SN2>," + randString + hexIV.substring(13,26) + ",<EOF>";
```

```
String innerEncryptedMessageA = Encryptb(true, tempA, K2, N2);
String HexinnerEncryptedMessageA = innerEncryptedMessageA;
String innerEncryptedMessageB = Encryptb(true, tempB, K2, N2);
String HexinnerEncryptedMessageB = innerEncryptedMessageB;
String innerEncryptedMessageC = Encryptb(true, tempC, K2, N2);
String HexinnerEncryptedMessageC = innerEncryptedMessageC;
String innerEncryptedMessageD = Encryptb(true, tempD, K2, N2);
String HexinnerEncryptedMessageD = innerEncryptedMessageD;
String innerEncryptedMessageE = Encryptb(true, tempE, K2, N2);
String HexinnerEncryptedMessageE = innerEncryptedMessageE;

//Have had to use @ instead of , as have used , to seperate hex values
    String temp2 = "<ETE>,@" + HomeID + "@" + HexinnerEncryptedMessageA + "@" +
    HexinnerEncryptedMessageB + "@" + HexinnerEncryptedMessageC + "@" +
    HexinnerEncryptedMessageD +  "@" + HexinnerEncryptedMessageE + "@,<EOF>";

byte[] outerEncryptedMessage = Encrypt(true, temp2, sessionKey, AESinitV);
String HexouterEncryptedMessage = new String(outerEncryptedMessage);

StringBuffer results = new StringBuffer();
String resultField = "No data recived";

try{

   streamConnection = (StreamConnection) Connector.open(connectString);
   outputStream = streamConnection.openOutputStream();
   dataOutputStream = new DataOutputStream(outputStream);

   System.out.println("TCP Connection Established");

   int x = 0;

   while(x < (outerEncryptedMessage.length) ){
      dataOutputStream.writeByte(outerEncryptedMessage[x]);
      x++;
   }


   //Prints a comma to seperate parameters
   dataOutputStream.writeByte(44);

   //Prints <EOF> at the end of string to end conection
   dataOutputStream.writeByte(60);
   dataOutputStream.writeByte(69);
   dataOutputStream.writeByte(79);
   dataOutputStream.writeByte(70);
   dataOutputStream.writeByte(62);

   dataOutputStream.flush();

}catch(IOException e){
   System.err.println("Exception Caught:" + e);
}finally{

      try{
         if(dataInputStream != null){
         dataInputStream.close();
         }
```

```
            }catch(IOException ignored){};

            try{
               if(dataOutputStream != null){
               dataOutputStream.close();
               }
            }catch(IOException ignored){};

            try{
               if(outputStream != null){
               outputStream.close();
               }
            }catch(IOException ignored){};

            try{
                if(inputStream != null){
               inputStream.close();
               }
            }catch(IOException ignored){};

            try{
                if(streamConnection != null){
               streamConnection.close();
               }
            }catch(IOException ignored){};
      }

      String data = new String("Done");
      return data;

   }

////////////////////////////////////////////////////////////////////////////////
////////////////////////////////////////////////////////////////////////////////

////////////////////////////////////////////////////////////////////////////////
//The encryption function used to encrypt data                                //
////////////////////////////////////////////////////////////////////////////////

public byte[] EncryptByte(boolean Encrypt, byte[] rawData){

            CCMBlockCipher ccm  = new CCMBlockCipher(new AESEngine());

      try{
            byte[] message = rawData;
            ccm.init(true, new ParametersWithIV(new KeyParameter(K1), N1));
            enc = new byte[message.length + 8];
            len = ccm.processBytes(message, 0, message.length, enc, 0);
            len += ccm.doFinal(enc, len);

      }catch(InvalidCipherTextException e){
         encryptedData = "error";
      }

         byte encryptedData [] = Hex.encode(enc);
         return encryptedData;

   }
```

```
////////////////////////////////////////////////////////////////////////////////////
////////////////////////////////////////////////////////////////////////////////////


////////////////////////////////////////////////////////////////////////////////////
//The decryption function used to decrypt data                                    //
////////////////////////////////////////////////////////////////////////////////////

public String Decrypt_v2(boolean Encrypt, String cipher){
System.out.println("Decryption Started");
        String test = "";

        cipher = cipher.trim();

        CCMBlockCipher ccm  = new CCMBlockCipher(new AESEngine());

        ccm.init(false, new ParametersWithIV(new KeyParameter(K1), N1));

           try{
              byte[] enc = new byte[100];
              enc = Hex.decode(cipher);
              byte[] tmp = new byte[enc.length];
              len = ccm.processBytes(enc, 0, enc.length, tmp, 0);
              len += ccm.doFinal(tmp, len);
              byte dec[] = new byte[len];
              System.arraycopy(tmp, 0, dec, 0, len);
              int i = 0;
              int judgement = 0;

              while(i < dec.length){
                 if(dec[i] == 44){
                    i=i+1;
                    test = test + Integer.toHexString(44);
                 }else{
                    if(dec[i+1] != 44){
                       int sum = 0;

                          if(dec[i] >= 48 && dec[i] <=57){
                             sum = sum + (dec[i]-48)*16;
                          }

                          if(dec[i] >= 65 && dec[i] <=70){
                             sum = sum + (dec[i]-55)*16;
                          }

                          if(dec[i] >= 97 && dec[i] <=102){
                             sum = sum + (dec[i]-87)*16;
                          }

                          if(dec[i+1] >= 48 && dec[i+1] <=57){
                             sum = sum + (dec[i+1]-48);
                          }

                          if(dec[i+1] >= 65 && dec[i+1] <=70){
                             sum = sum + (dec[i+1]-55);
                          }

                          if(dec[i+1] >= 97 && dec[i+1] <=102){
                             sum = sum + (dec[i+1]-87);
```

```
                    }

                        if(sum >= 0 && sum <= 15){

                        test = test + "" + "0" + Integer.toHexString(sum);

                        }else{
                            test = test + "" + Integer.toHexString(sum);
                        }

                    i=i+2;

                }else{

                int sum = 0;

                    if(dec[i] >= 48 && dec[i] <=57){
                        sum = sum + (dec[i]-48);
                    }

                    if(dec[i] >= 65 && dec[i] <=70){
                        sum = sum + (dec[i]-55);
                    }

                    if(dec[i] >= 97 && dec[i] <=102){
                        sum = sum + (dec[i]-87);
                    }

                        if(sum >= 0 && sum <= 15){

                        test = test + "" + "0" + Integer.toHexString(sum);

                        }else{
                            test = test + "" + Integer.toHexString(sum);
                        }

                    i=i+1;
                }
            }
          }

        }catch(InvalidCipherTextException e){
            test = "Error: Decryption Failed";
        }

      test.trim();
      return test;
    }

////////////////////////////////////////////////////////////////////////////////
////////////////////////////////////////////////////////////////////////////////


////////////////////////////////////////////////////////////////////////////////
//Code used to generate AES session keys                                      //
////////////////////////////////////////////////////////////////////////////////

   public void generateAESKey() throws Exception {
```

```
    SecureRandom sr = new SecureRandom();

    sessionKey2 = new byte[16];
    sr.nextBytes(sessionKey2);
    AESinitV2 = new byte[13];
    sr.nextBytes(AESinitV2);

  }

////////////////////////////////////////////////////////////////////////////////
////////////////////////////////////////////////////////////////////////////////
```

RHS-2 Approach, Mobile Client Source Code

```
////////////////////////////////////////////////////////////////////////////////
// Local Variables                                                            //
//These variables are similar to those for the RHS-1 approach ,      //
//however the home IP address is left empty, for input by the RHS //
////////////////////////////////////////////////////////////////////////////////

private StreamConnection streamConnection = null;
private OutputStream outputStream = null;
private DataOutputStream dataOutputStream = null;

private InputStream inputStream = null;
private DataInputStream dataInputStream = null;

private String connectString = "socket://192.168.0.102:11000";
private String connectStringHome = "socket://0.0.0.0:2101";

//The hex decode function converts the hex key and IV into their dec equivalent

private byte[] K1 = Hex.decode("404142434445464748494a4b4c4d4e4f");
private byte[] N1 = Hex.decode("101112131415161718191a1b1c");

private byte[] K2 = Hex.decode("303132333435363738393a3b3c3d3e3f");
private byte[] N2 = Hex.decode("202122232425262728292a2b2c");

private byte [] sessionKey;
private byte [] AESinitV;
private int randomNumber;
private int randomNumberHome;

private byte [] sessionKey2;
private byte [] AESinitV2;
private int randomNumber2;

////////////////////////////////////////////////////////////////////////////////
////////////////////////////////////////////////////////////////////////////////




////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////
//The login code – during the home.login function discussed later the homes IP address is          //
```

```
//retrieved from the RHS and a direct connection to the WSN based HAS is made                    //
////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////

  public void login(String userName, String userPassword){

          String loginStatus = Home.login(userName, userPassword);

          if(!loginStatus.equals("-1")){

            String data = "";
            String testData = "";
           HomeID = loginStatus;

            System.out.println(HomeID);

            MainMenu();

             //Load the local database with sensor readings
             sensorDatabase();

         }else if(loginStatus.equals("-1")){
             loginStatuslbl.setText("The login detailes you provided were incorrect, please try
again.\n\n ");
         }else{
         message("Critical Login Error Recived: " + loginStatus);
         }
 }

////////////////////////////////////////////////////////////////////////////////
////////////////////////////////////////////////////////////////////////////////

////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////
//The login function encrypts the user username and password and sends it to the RHS for          //
//authentication, the RHS responds with the IP address of the WSN based HAS. After this point    //
//the mobile communicates directly with the WSN based HAS. The encryption function for the       //
//RHS-2 approach and the RHS-1 approach are the same, consequently it is not repeated hear.      //
////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////

public String login(String userName, String userPassword){


       StringBuffer results = new StringBuffer();
       String resultField = "No data recived";
       randomNumberHome = 10;


       try{

          streamConnection = (StreamConnection) Connector.open(connectString);
          outputStream = streamConnection.openOutputStream();
          dataOutputStream = new DataOutputStream(outputStream);

          byte[] byteMessage = Encrypt(true,("<lgn>" + "," + userName + "," + userPassword + "," +
"<EOF>"),K1,N1);

          int x = 0;

          while(x < (byteMessage.length) ){
             dataOutputStream.writeByte(byteMessage[x]);
```

```
            //System.out.println(byteMessage[x]);
            x++;
        }

        //Prints a comma
        dataOutputStream.writeByte(44);

        //Prints <EOF> at the end of string to end conection
        dataOutputStream.writeByte(60);
        dataOutputStream.writeByte(69);
        dataOutputStream.writeByte(79);
        dataOutputStream.writeByte(70);
        dataOutputStream.writeByte(62);

        dataOutputStream.flush();

        inputStream = streamConnection.openInputStream();
        dataInputStream = new DataInputStream(inputStream);

        int inputChar;

        while((inputChar = dataInputStream.read()) != -1){
            //System.out.println("test: " + (char)inputChar);
            results.append((char) inputChar);
        }

        resultField = new String(results.toString());

        dataInputStream.close();

    }catch(IOException e){
        System.err.println("Exception Caught:" + e);
    }finally{

        try{
            if(dataInputStream != null){
            dataInputStream.close();
            }
        }catch(IOException ignored){};

        try{
            if(dataOutputStream != null){
            dataOutputStream.close();
            }
        }catch(IOException ignored){};

        try{
            if(outputStream != null){
            outputStream.close();
            }
        }catch(IOException ignored){};

        try{
             if(inputStream != null){
            inputStream.close();
            }
        }catch(IOException ignored){};

        try{
```

```
                if(streamConnection != null){
                streamConnection.close();
                }
            }catch(IOException ignored){};
        }


        String loginStatus = resultField.trim();

        return loginStatus;


    }

////////////////////////////////////////////////////////////////////////////////////
////////////////////////////////////////////////////////////////////////////////////
```